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 janvier 2008
N° CERTA-2008-AVI-009

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités protocolaires dans Microsoft Windows

Gestion du document

Référence	CERTA-2008-AVI-009
Titre	Vulnérabilités protocolaires dans Microsoft Windows
Date de la première version	09 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-001 du 08 janvier 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 ;
- Windows XP Professional x64 Edition ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 1 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 pour systèmes Itanium (SP1 et SP2) ;
- Windows Vista ;
- Windows Vista x64 Edition.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans la mise en œuvre par le noyau Windows de certains protocoles. Ces vulnérabilités peuvent être exploitées à distance, par le biais de trames spécialement construites, afin de perturber le système vulnérable, voire d'y exécuter des commandes arbitraires.

4 Description

Plusieurs vulnérabilités ont été identifiées dans la mise en œuvre par le noyau Windows de certains protocoles.

1. le noyau Windows ne stockerait pas correctement les informations issues de requêtes IGMPv3 et MLDv2. `IGMP` (pour *Internet Group Management Protocol*) est un protocole utilisé pour signaler les appartenances de groupes de diffusion, ou *multicast*, sous IPv4. `MLDv2` (pour *Multicast Listener Discovery*) est un protocole utilisé par les routeurs sous IPv6 pour découvrir les nœuds intéressés par la diffusion, ou *multicast*, et les adresses candidates. Il se définit comme un dérivé du protocole `ICMPv6`.
2. le noyau Windows ne manipulerait pas correctement les requêtes de découverte au niveau du routage par le protocole ICMP `RDP` (*Router Discovery Protocol*). Ce protocole n'est cependant pas activé par défaut.

Ces vulnérabilités peuvent être exploitées à distance, par le biais de trames spécialement construites, afin de perturber le système vulnérable, voire d'y exécuter des commandes arbitraires.

5 Solution

Se référer au bulletin de sécurité MS08-001 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-001 du 08 janvier 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-001.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-001.mspx
- Référence CVE CVE-2007-0066 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0066
- Référence CVE CVE-2007-0069 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0069
- RFC 3376, "Internet Group Management Protocol, Version 3", octobre 2002 :
  http://www.ietf.org/rfc/rfc3376.txt
- RFC 3810, "Multicast Listener Discovery Version 2 (MLDv2) pour IPv6", juin 2004 :
  http://www.ietf.org/rfc/rfc3810.txt

Gestion détaillée du document

09 janvier 2008 version initiale.