Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juin 2008
N° CERTA-2008-AVI-306

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités protocolaires dans Windows (PGM)

Gestion du document

Référence	CERTA-2008-AVI-306
Titre	Vulnérabilités protocolaires dans Windows (PGM)
Date de la première version	11 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-036 du 10 juin 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Windows XP Service Pack 2 ;
- Windows XP Service Pack 3 ;
- Windows XP x64 Edition ;
- Windows XP x64 Edition Service Pack 2 ;
- Windows Vista ;
- Windows Vista Service Pack 1 ;
- Windows Vista x64 Edition ;
- Windows Vista x64 Edition Service Pack 1 ;
- Windows 2003 Server Service Pack 1 ;
- Windows 2003 Server Service Pack 2 ;
- Windows 2003 Server x64 Edition ;
- Windows 2003 Server x64 Edition Service Pack 2 ;

– Windows 2003 Server (SP1 et SP2) pour systèmes Itanium ;
– Windows 2008 Server (pour systèmes 32-bit, x64 et Itanium).

3 Résumé

Deux vulnérabilités ont été identifiées dans la mise en œuvre du protocole PGM (*Pragmatic General Multicast*) du système d'exploitation Windows. Elles peuvent être exploitées par des personnes malveillantes distantes afin de perturber le fonctionnement du système et en particulier ses communications réseau.

4 Description

Deux vulnérabilités ont été identifiées dans la mise en œuvre du protocole PGM (*Pragmatic General Multicast*) du système d'exploitation Windows : elles concernent le champ précisant la longueur des options et l'option de fragmentation.

Ce protocole peut être utilisé pour la diffusion en groupes ou *multicast* et s'appuie sur le principe des accusés de réception négatifs (`NACK`) pour signaler des données qui n'ont pas été reçues. Il porte le numéro protocolaire 113 dans l'en-tête IP. Il n'est pas activé par défaut. Il peut cependant l'être si le service `MSMQ` (pour *Microsoft Message Queuing* est installé par exemple.

Une personne malveillante distante peut exploiter l'une de ces vulnérabilités par le biais de trames spécialement construites afin de perturber les échanges réseau du système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS08-036 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité Microsoft MS08-036 du 10 juin 2008 :
http://www.microsoft.com/france/technet/security/Bulletin/MS08-036.mspx
http://www.microsoft.com/technet/security/Bulletin/MS08-036.mspx
– Bloc-notes de Microsoft détaillant le protocole PGM :
http://blogs.technet.com/swi/archive/2008/06/10/ms08-036-pgm-what-is-pgm.aspx
– RFC 3208, "PGM Reliable Transport Protocol Specification", décembre 2001 :
http://www.ietf.org/rfc/rfc3208.txt
– Référence CVE CVE-2008-1440 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1440
– Référence CVE CVE-2008-1441 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1441

Gestion détaillée du document

11 juin 2008 version initiale.