Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2006
N° CERTA-2006-AVI-387

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole PGM dans Microsoft Windows

Gestion du document

Référence	CERTA-2006-AVI-387
Titre	Vulnérabilité du protocole PGM dans Microsoft Windows
Date de la première version	13 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS06-052 de Microsoft publié le 12 septembre 2006
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

Le service MSMQ (*Microsoft Message Queuing*) 3.0 pour :
– Windows XP Service Pack 1 et Service Pack 2
La version *Edition x64* de ce système d'exploitation ne serait pas affectée par cette vulnérabilité.

3 Résumé

Une vulnérabilité a été identifiée dans le protocole PGM (*Pragmatic General Multicast*), utilisé notamment par le service MSMQ (pour *Microsoft Message Queuing*). Ce service n'est pas installé ou activé par défaut. Une personne malveillante pourrait envoyer un paquet conçu dans le but d'exploiter cette vulnérabilité via le protocole PGM. Cela lui permettrait d'exécuter des commandes arbitraires, au moment de la réception du paquet par le système vulnérable.

4 Description

Le transport *multicast* permet de diffuser simultanément de l'information à un groupe restreint de machines. Au niveau d'IPv4, les adresses réservées pour ce dernier sont dans la plage 224.0.0.0/4 (224.0.0.0 à 239.255.255.255).

Il existe plusieurs implémentations de protocoles *multicast*, l'une d'elles étant le `PGM` (pour *Pragmatic General Multicast*). Elle est définie par la norme RFC 3208 et s'appuie sur le principe des accusés de réception négatifs (`NACK`), pour signaler des données qui n'ont pas été reçues. `PGM` est un protocole de la couche transport, par analogie avec TCP ou UDP, et porte le numéro de protocole 113 dans l'entête IPv4.

Les versions actuelles de Microsoft Windows ne mettent pas en œuvre ce protocole par défaut. En revanche, `PGM` peut être activé si le service `MSMQ` (pour *Microsoft Message Queuing*) est installé.

Une vulnérabilité a été identifiée dans la mise en œuvre du protocole `PGM` pour certaines versions de Microsoft Windows, permettant un accès illégitime à la mémoire. Une personne malveillante pourrait envoyer un paquet conçu dans le but d'exploiter cette vulnérabilité. Cela lui permettrait d'exécuter des commandes arbitraires, au moment de la réception du paquet par le système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS06-052 de Microsoft pour l'application des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-052 du 12 septembre 2006 :
  http://www.microsoft.com/france/technet/security//bulletin/2006/MS06-052.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-052.mspx
- Référence CVE CVE-2006-3442 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3442

Gestion détaillée du document

13 septembre 2006 version initiale.