Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2010
N° CERTA-2010-AVI-070

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Windows SMB

Gestion du document

Référence	CERTA-2010-AVI-070
Titre	Multiples vulnérabilités dans Microsoft Windows SMB
Date de la première version	10 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS10-012 du 09 février 2010
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et Windows XP Service Pack 3 ;
- Microsoft Windows XP Professionnel Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Microsoft Windows Vista, Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Microsoft Windows Vista Édition x64, Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;

- Microsoft Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Microsoft Windows 7 pour systèmes 32 bits ;
- Microsoft Windows 7 pour systèmes x64 ;
- Microsoft Windows Server 2008 R2 pour systèmes x64;
- Microsoft Windows Server 2008 R2 pour systèmes Itanium.

3 Résumé

Plusieurs vulnérabilités dans `Microsoft Windows SMB` permettent, entre autre, à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités dans `Microsoft Windows SMB` ont été découvertes :

- une erreur dans le traitement de paquets *SMB* (*Server Message Block*) permet à un utilisateur authentifié d'exécuter du code arbitraire à distance (CVE-2010-0020) ;
- des erreurs dans le traitement de paquets *SMB* (*Server Message Block*) permettent à une personne distante non authentifiée de provoquer un déni de service (CVE-2010-0021 et CVE-2010-0022) ;
- une erreur dans le traitement des authentifications *SMB* (*Server Message Block*) permet à une personne non authentifiée d'élever ses privilèges sur le système (CVE-2010-0231).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS10-012 du 09 février 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-012.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-012.mspx
- Référence CVE CVE-2010-0020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0020
- Référence CVE CVE-2010-0021 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0021
- Référence CVE CVE-2010-0022 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0022
- Référence CVE CVE-2010-0231 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0231

Gestion détaillée du document

10 février 2010 version initiale.