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 janvier 2009
N° CERTA-2009-AVI-012

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités de SMB dans Windows

Gestion du document

Référence	CERTA-2009-AVI-012
Titre	Plusieurs vulnérabilités de SMB dans Windows
Date de la première version	13 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-001 du 13 janvier 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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP (SP2 et SP3), y compris la version x64 Edition ;
- Windows Server 2003 (SP1 et SP2), y compris les versions x64 Edition ou pour systèmes Itanium ;
- Windows Vista et Windows Vista SP1, y compris la version x64 Edition ;
- Windows Server 2008 pour les systèmes 32-bit, x64 ou Itanium.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans la mise en œuvre de SMB sous Windows. L'exploitation de ces dernières par une personne malveillante distante peut permettre dans certaines conditions d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Trois vulnérabilités ont été identifiées dans la mise en œuvre de SMB (*Microsoft Server Message Block*) sous Windows. Aucune ne nécessite d'authentification préalable. Leur exploitation peut conduire à un déni de service du système vulnérable distant, voire à l'exécution de code arbitraire.

5 Solution

Se référer au bulletin de sécurité MS09-001 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-001 du 13 janvier 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-001.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-001.mspx
- Référence CVE CVE-2008-4114 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4114
- Référence CVE CVE-2008-4834 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4834
- Référence CVE CVE-2008-4835 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4835

Gestion détaillée du document

13 janvier 2009 version initiale.