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-064

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le client SMB de Microsoft Windows

Gestion du document

Référence	CERTA-2010-AVI-064
Titre	Vulnérabilités dans le client SMB de Microsoft Windows
Date de la première version	10 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-006 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 ;
- élévation de privilèges.

2 Systèmes affectés

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

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

3 Résumé

Deux vulnérabilités permettant l'exécution de code arbitraire à distance ont été corrigées dans le client `SMB` de `Microsoft Windows`.

4 Description

Deux vulnérabilités dans le client `SMB` de `Microsoft Windows` ont été corrigées. Leur exploitation peut permettre à un attaquant d'exécuter du code arbitraire à distance en envoyant une réponse `SMB` spécialement conçue à une requête `SMB` établie par le client.

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 MS10-006 du 09 février 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-006.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-006.mspx
- Référence CVE CVE-2010-0016 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0016
- Référence CVE CVE-2010-0017 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0017

Gestion détaillée du document

10 février 2010 version initiale.