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 avril 2011
N° CERTA-2011-AVI-202

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le client SMB de Microsoft

Gestion du document

Référence	CERTA-2011-AVI-202
Titre	Vulnérabilités dans le client SMB de Microsoft
Date de la première version	13 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-019 du 12 avril 2011
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 XP Service Pack 3 ;
- Microsoft Windows XP Professional x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 SP2 pour les systèmes Itanium ;
- Microsoft Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Microsoft Windows Vista x64 Edition Service Pack 1 et Windows Vista x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2008 et Windows Server 2008 Service Pack 2 pour les systèmes 32-bit ;
- Microsoft Windows Server 2008 et Windows Server 2008 Service Pack 2 pour les systèmes x64 ;
- Microsoft Windows Server 2008 et Windows Server 2008 Service Pack 2 pour les systèmes Itanium ;
- Microsoft Windows 7 pour les systèmes 32-bit et Service Pack 1 ;
- Microsoft Windows 7 pour les systèmes x64 et Service Pack 1 ;
- Microsoft Windows Server 2008 R2 pour les systèmes x64 et Service Pack 1;
- Microsoft Windows Server 2008 R2 pour les systèmes Itanium et Service Pack 1.

3 Résumé

Deux vulnérabilités découvertes dans le client SMB de Microsoft permettent à une personne malveillante d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités causées par une erreur dans le traitement de certains paquets SMB (*Server Message Block*) ou CIFS (*Common Internet File System*), peuvent être exploitées sans authentification afin d'exécuter du code arbitraire.

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 MS11-019 du 12 avril 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-019.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-019.mspx
- Référence CVE CVE-2011-0654 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0654
- Référence CVE CVE-2011-0660 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0660

Gestion détaillée du document

13 avril 2011 version initiale.