Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 octobre 2009
N° CERTA-2009-ALE-016-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de SMBv2 dans Microsoft Windows

Gestion du document

Référence	CERTA-2009-ALE-016-002
Titre	Vulnérabilité de SMBv2 dans Microsoft Windows
Date de la première version	09 septembre 2009
Date de la dernière version	14 octobre 2009
Source(s)	Avis de sécurité Microsoft 975497 du 08 septembre 2009 Bulletin de sécurité Microsoft MS09-050 du 13 octobre 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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Windows Vista ;
- Microsoft Windows Vista Service Pack 1 ;
- Microsoft Windows Vista Service Pack 2 ;
- Microsoft Windows Vista x64 ;
- Microsoft Windows Vista x64 Service Pack 1 ;
- Microsoft Windows Vista x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits ;
- Microsoft Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes Itanium ;
- Microsoft Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes x64 ;
- Microsoft Windows Server 2008 pour systèmes x64 Service Pack 2.

3 Résumé

Une vulnérabilité dans SMBv2 sous Microsoft Windows permet à une personne malintentionnée distante de provoquer un déni de service et potentiellement d'exécuter du code arbitraire.

4 Description

Une vulnérabilité a été identifiée dans le pilote srv2.sys. Une personne malintentionnée distante, peut, au moyen d'un paquet spécifiquement conçu, provoquer un déni de service voire exécuter du code arbitraire.

Du code d'exploitation est disponible sur l'Internet.

5 Contournement provisoire

- désactiver SMB v2 (cf. avis Microsoft) ;
- filtrer les ports 139/TCP et 445/TCP en amont.

Les contournements proposés permettent de maintenir la mise en œuvre du partage de fichiers en utilisant le protocole SMB dans sa version 1.

Toutefois des effets de bords liés à l'application de ces contournements ne peuvent être écartés, telle une diminution des performances. De ce fait, le CERTA recommande de procéder à la vérification de ces contournements dans le contexte du système d'information vulnérable avant tout déploiement.

De plus, Microsoft a publié deux outils permettant d'automatiser l'application du contournement provisoire ainsi que son retrait. Ces outils sont disponibles à l'adresse suivante :

http://support.microsoft.com/kb/975497

6 Solution

Le bulletin de sécurité MS09-050 de Microsoft corrige cette vulnérabilité.

7 Documentation

- Bulletin de sécurité Microsoft MS09-050 du 13 octobre 2009 :
  http://www.microsoft.com/technet/security/bulletin/ms09-050.mspx
- Référence CVE CVE-2009-3103 :
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-3103
- Avis de sécurité Microsoft 975497 du 08 septembre 2009 :
  http://www.microsoft.com/technet/security/advisory/975497.mspx
- Article Microsoft 975497 du 17 septembre 2009 :
  http://support.microsoft.com/kb/975497

Gestion détaillée du document

09 septembre 2009 version initiale ;

18 septembre 2009 ajout d'un lien dans la section Documentation et modification de la section Contournement provisoire ;

13 octobre 2009 ajout du correctif.