



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 octobre 2008
N° CERTA-2008-AVI-504

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité SMB dans Microsoft Windows

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-504>

Gestion du document

Référence	CERTA-2008-AVI-504
Titre	Vulnérabilité SMB dans Microsoft Windows
Date de la première version	15 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-063 du 14 octobre 2008
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 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Microsoft XP Professional x64 Edition ;
- Microsoft XP Professional x64 Edition Service Pack 2 ;
- Windows Vista ;
- Windows Vista Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 SP1 et SP2 pour systèmes Itanium ;
- Microsoft Windows Server 2008 (systèmes 32-bit et x64, y compris pour systèmes Itanium).

3 Résumé

Une vulnérabilité a été identifiée dans la mise en œuvre protocolaire *Microsoft Server Message Block* (SMB). Elle pourrait être exploitée à distance par le biais d'une trame spécialement construite. L'exploitation de cette vulnérabilité peut conduire à l'exécution de code arbitraire sur le poste distant vulnérable.

4 Description

Une vulnérabilité a été identifiée dans la mise en œuvre protocolaire *Microsoft Server Message Block* (SMB). Les noms de fichiers ne seraient pas correctement vérifiés.

Qualifiée d' « importante » plutôt que « critique » par Microsoft, cette vulnérabilité pourrait être exploitée à distance par le biais d'une trame spécialement construite et conduire à l'exécution de code arbitraire sur le poste vulnérable.

5 Solution

Se référer au bulletin de sécurité MS08-063 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-063 du 14 octobre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-063.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-063.msp>
- Référence CVE CVE-2008-4038 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4038>

Gestion détaillée du document

15 octobre 2008 version initiale.