



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2008
N° CERTA-2008-AVI-549

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-549>

Gestion du document

Référence	CERTA-2008-AVI-549
Titre	Vulnérabilité de SMB dans Microsoft Windows
Date de la première version	12 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-068 du 11 novembre 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 et Service Pack 3 ;
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 compris) ;
- Microsoft Windows Server 2003 Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition (Service Pack 2 compris) ;
- Microsoft Windows Server 2003 pour systèmes Itanium (SP1 et SP2) ;
- Microsoft Windows Vista (Service Pack 1 compris) ;
- Microsoft Windows Server 2008 pour systèmes 32-bit, x64 et Itanium.

3 Résumé

Une vulnérabilité a été identifiée dans la mise en oeuvre du protocole SMB de Windows. L'exploitation de cette dernière peut provoquer, sous certaines conditions, l'exécution de code arbitraire sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans la mise en oeuvre du protocole *Microsoft Server Message Block* (SMB) de Windows. Elle permettrait à une personne malveillante de rediriger une tentative de connexion SMB vers la machine émettrice puis exploiter les crédits d'authentification pour s'y connecter (technique aussi appelée "*credential reflection*").

L'exploitation de cette vulnérabilité permet donc, sous certaines conditions, d'exécuter du code arbitraire sur le système vulnérable. Du code d'exploitation est actuellement disponible sur l'Internet.

5 Solution

Se référer au bulletin de sécurité MS08-068 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-068 du 11 novembre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-068.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-068.msp>
- Bloc-notes de Microsoft, "*MS08-068: SMB credential reflection defense*" publié le 11 novembre 2008 :
<http://blogs.technet.com/swi/archive/2008/11/11/smb-credential-reflection.aspx>
- Référence CVE CVE-2008-4037 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4037>

Gestion détaillée du document

12 novembre 2008 version initiale.