



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 novembre 2009
N° CERTA-2009-ALE-019

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Windows 7 et Windows Server 2008 R2

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-2009-ALE-019>

Gestion du document

Référence	CERTA-2009-ALE-019
Titre	Vulnérabilité dans Windows 7 et Windows Server 2008 R2
Date de la première version	16 novembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft 977544 du 13 novembre 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

Déni de service à distance.

2 Systèmes affectés

- Windows 7 ;
- Windows 7 pour systèmes 64 bits ;
- Windows Server 2008 R2 pour systèmes 64 bits ;
- Windows Server 2008 R2 pour systèmes Itanium.

3 Résumé

Une vulnérabilité dans Windows 7 et Windows Server 2008 R2 permet à une personne distante d'effectuer un déni de service.

4 Description

Une vulnérabilité affectant l'implémentation du protocole *SMB (Server Message Block)* dans *Windows 7* et *Windows Server 2008 R2* permet à une personne malintentionnée distante de provoquer un déni de service. Le savoir-faire permettant d'exploiter cette vulnérabilité a été publié sur l'Internet.

5 Contournement provisoire

En attendant la publication d'un correctif par l'éditeur, le CERTA recommande de mettre en place la mesure suivante : filtrer les ports *TCP/139* et *TCP/445*.

Le filtrage de ces ports peut nuire au fonctionnement de diverses applications ou services comme le partage de fichiers et d'imprimantes, les politiques de groupe, *Distributed File System (DFS)*, ...

6 Documentation

- Bulletin de sécurité Microsoft 977544 du 13 novembre 2009 :
<http://www.microsoft.com/technet/security/advisory/977544.mspx>
- Référence CVE CVE-2009-3676 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676>

Gestion détaillée du document

16 novembre 2009 version initiale.