

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le client SMB de Microsoft

---

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-2011-AVI-351>

---

### Gestion du document

Référence	CERTA-2011-AVI-351-001
Titre	Vulnérabilité dans le client SMB de Microsoft
Date de la première version	15 juin 2011
Date de la dernière version	24 juin 2011
Source(s)	Bulletin de sécurité Microsoft MS11-043 du 14 juin 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

- Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 with SP2 pour systèmes Itanium ;
- Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 1 et Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 pour systèmes 32-bit et Windows Server 2008 pour systèmes 32-bit Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium and Windows Server 2008 systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32-bit ;
- Windows 7 pour systèmes 32-bit Service Pack 1 ;
- Windows 7 pour systèmes x64 ;

- Windows 7 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes x64 Systems ;
- Windows Server 2008 R2 pour systèmes x64 Systems Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium ;
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

### 3 Résumé

Une vulnérabilité dans le client SMB de Microsoft permet à une personne malveillante d'exécuter du code arbitraire à distance.

### 4 Description

Une vulnérabilité, causée par une erreur dans le traitement de paquet SMB, permet à un individu malintentionné d'exécuter du code arbitraire à distance au moyen d'une réponse SMB spécialement construite et sans authentification préalable.

L'éditeur met en garde contre des incompatibilités entre l'application du correctif et certaines configurations du serveur SAMBA. Il a mis à jour le bulletin KB2536276 à cet effet dans sa base de support (cf. section Documentation).

### 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 MS11-043 du 14 juin 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-043.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-043.msp>
- Bulletin de support Microsoft KB2536276 du 22 juin 2011 :  
<http://support.microsoft.com/kb/2536276/en-us>
- Référence CVE CVE-2011-1268 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1268>

### Gestion détaillée du document

**15 juin 2011** version initiale.

**24 juin 2011** ajout d'effets secondaires possibles.