

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-2005-AVI-058>

Gestion du document

Référence	CERTA-2005-AVI-058
Titre	Vulnérabilité de SMB dans Microsoft Windows
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-011
Pièce(s) jointe(s)	

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 3 & 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP 64-bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 pour systèmes Itanium.

3 Résumé

Une vulnérabilité présente dans certaines versions de Microsoft Windows permet à un individu mal intentionné d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Server Message Block (SMB) est un protocole utilisé sous Microsoft Windows pour le partage de ressources disque et pour la communication entre clients à l'aide de fichiers spéciaux (les tubes nommés par exemple).

Une vulnérabilité découverte dans le protocole Server Message Block permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur le système vulnérable en incitant une victime à cliquer sur un lien malicieusement constitué présent dans un mail ou au moyen de requêtes malicieusement construites à condition d'être sur le même sous-réseau.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS05-011 du 08 février 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-011.mspx>
- Référence CVE CAN-2005-0045 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0045>

Gestion détaillée du document

09 février 2005 version initiale.