

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2010-AVI-168>

Gestion du document

Référence	CERTA-2010-AVI-168
Titre	Vulnérabilités dans le client SMB de Microsoft
Date de la première version	14 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-020 du 13 avril 2010
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 ;
- déni de service à distance.

2 Systèmes affectés

Windows et Windows Server, toutes les versions et toutes les architectures.

3 Résumé

Plusieurs vulnérabilités affectent le client SMB de Microsoft, permettant à un utilisateur malveillant distant de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent le client SMB de Microsoft :

- un problème dans la gestion des réponses incomplètes permet à un utilisateur distant non authentifié de bloquer le système vulnérable, obligeant au redémarrage de celui-ci ;

- quatre problèmes dans le traitement des paquets SMB sont exploitables par un utilisateur malveillant non authentifié pour exécuter du code arbitraire à distance.

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 MS10-020 du 13 avril 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-020.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-020.msp>
- Référence CVE CVE-2009-3676 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676>
- Référence CVE CVE-2010-0269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0269>
- Référence CVE CVE-2010-0270 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0270>
- Référence CVE CVE-2010-0476 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0476>
- Référence CVE CVE-2010-0477 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0477>

Gestion détaillée du document

14 avril 2010 version initiale.