

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le seueur SMB de 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-2010-AVI-370>

Gestion du document

Référence	CERTA-2010-AVI-370
Titre	Multiples vulnérabilités dans le seueur SMB de Microsoft Windows
Date de la première version	11 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-054 du 10 août 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

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

- Microsoft Windows Server 2008 R2 pour les systèmes x64 ;
- Microsoft Windows Server 2008 R2 pour les systèmes Itanium.

3 Résumé

Plusieurs vulnérabilités présentes dans le serveur SMB de Microsoft Windows permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Trois vulnérabilités sont présentes dans le serveur SMB de Microsoft Windows. Deux d'entre elles (CVE-2010-2551 et CVE-2010-2552) permettent à un utilisateur distant malintentionné de provoquer un déni de service. La dernière (CVE-2010-2550) permet à un utilisateur distant non-authentifié malintentionné d'exécuter du code arbitraire.

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 MS10-054 du 10 août 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-054.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-054.mspx>
- Référence CVE CVE-2010-2550 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2550>
- Référence CVE CVE-2010-2551 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2551>
- Référence CVE CVE-2010-2552 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2552>

Gestion détaillée du document

11 août 2010 version initiale.