

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le partage de cluster de disques sous Windows Server

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-496>

Gestion du document

Référence	CERTA-2010-AVI-496
Titre	Vulnérabilité dans le partage de cluster de disques sous Windows Server
Date de la première version	13 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-086 du 12 octobre 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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

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

3 Résumé

Une vulnérabilité dans le partage de *cluster* de disques, sous Windows Server 2008 R2, peut être utilisée par un utilisateur malintentionné pour porter atteinte à l'intégrité et à la confidentialité des données.

4 Description

Une vulnérabilité existe dans la gestion des *clusters* de disques partagés sous Windows Server 2008 R2. Cette vulnérabilité s'applique uniquement au *cluster* de disques de basculement. Lors de l'ajout d'un disque,

le gestionnaire du *cluster* de basculement met des autorisations par défauts pouvant permettre, à un utilisateur malintentionné, de porter atteinte à l'intégrité et à la confidentialité des données.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La mise à jour proposée par Microsoft corrige la façon dont sont définies les permissions par défaut, mais pas les permissions existantes sur les *clusters* de disques partagés. Les administrateurs devront donc vérifier les permissions sur les *clusters* de disques existants une fois la mise à jour appliquée.

6 Documentation

- Bulletin de sécurité Microsoft MS10-086 du 12 octobre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-086.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-086.msp>
- Référence CVE CVE-2010-3223 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3223>

Gestion détaillée du document

13 octobre 2010 version initiale.