

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les services SharePoint 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-2005-AVI-057>

Gestion du document

Référence	CERTA-2005-AVI-057
Titre	Vulnérabilités dans les services SharePoint de Microsoft
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-006 du 08 février 2005
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 Server 2003 pour les systèmes Itanium ;
- SharePoint Portal Server 2003 ;
- SharePoint Portal Server 2001.

3 Résumé

Deux vulnérabilités présentes dans le service SharePoint de Microsoft permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Microsoft SharePoint Portal Server permet la création de portail d'entreprise. Plusieurs sites peuvent être connectés au sein d'un même portail.

- La première vulnérabilité de type "Cross Site Scripting" permet à un utilisateur mal intentionné d'inciter sa victime à exécuter un code arbitraire sur son système avec ses privilèges.
- La seconde vulnérabilité permet à un utilisateur distant de polluer le cache du site web afin d'en modifier le contenu.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS05-006 du 08 février 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-006.msp>
- Référence CVE CAN-2005-0049 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0049>

Gestion détaillée du document

09 février 2005 version initiale.