



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 08 avril 2004
N° CERTA-2004-AVI-120

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft SharePoint Portal Server 2001

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-2004-AVI-120>

Gestion du document

Référence	CERTA-2004-AVI-120
Titre	Vulnérabilités dans Microsoft SharePoint Portal Server 2001
Date de la première version	08 avril 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft KB837017
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 scripts ;
- vol de cookies.

2 Systèmes affectés

Microsoft SharePoint Portal Server 2001.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans Microsoft SharePoint Portal Server 2001.

4 Description

Microsoft SharePoint Portal Server 2001 permet la création de portail d'entreprise. Plusieurs sites peuvent être connectés au sein d'un même portail.

Des vulnérabilités de type "Cross Site Scripting" permettent en utilisant Microsoft SharePoint Portal Server 2001 comme rebond d'exécuter des scripts malicieux sur une machine cible.

De plus il est possible par ce même type d'attaque de voler les cookies des utilisateurs visitant ces sites.

5 Solution

Télécharger le Service Pack3 qui corrige ces vulnérabilités (cf. Section Documentation).

6 Documentation

- Avis de sécurité de Microsoft KB837017 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=15677A92-3470-465F-9F63-E621094103E0>
- Référence CVE CAN-2004-0379 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0379>

Gestion détaillée du document

08 avril 2004 version initiale.