Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2010
N° CERTA-2010-AVI-482

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans SafeHTML

Gestion du document

Référence	CERTA-2010-AVI-482
Titre	Multiples vulnérabilités dans SafeHTML
Date de la première version	13 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-072 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

- Injection de code indirecte à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows SharePoint Services 3.0 Service Pack 2 (versions 32 bits) ;
- Microsoft Windows SharePoint Sevices 3.0 Service Pack 2 (versions 64 bits) ;
- Microsoft SharePoint Foundation 2010 ;
- Microsoft SharePoint Server 2007 Service Pack 2 (éditions 32 bits) ;
- Microsoft SharePoint Server 2007 Service Pack 2 (éditions 64 bits) ;
- Microsoft Groover Server 2010.

3 Résumé

Des vulnérabilités de type injection de code indirecte affectent notamment `Microsoft Share Point` et `Microsoft Share Point Services`.

4 Description

`Microsoft Share Point` et `Microsoft Share Point Services` utilisent *SafeHTML* afin d'assainir le contenu de formulaires HTML. Une vulnérabilité dans ce composant permet à un utilisateur distant malintentionné de réaliser une attaque par injection de code indirecte (*XSS*). Cette attaque peut mener à une atteinte à la confidentialité des données.

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 MS10-072 du 12 octobre 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-072.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-072.mspx
- Référence CVE CVE-2010-3243 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3243
- Référence CVE CVE-2010-3324 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3324

Gestion détaillée du document

13 octobre 2010 version initiale.