

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Sharepoint

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-2012-AVI-077>

Gestion du document

Référence	CERTA-2012-AVI-077
Titre	Vulnérabilités dans Microsoft Sharepoint
Date de la première version	15 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-011
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

- Élévation de privilèges ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Sharepoint Server 2010 et Service Pack 1 ;
- Microsoft Sharepoint Foundation 2010 et Service Pack 1.

3 Résumé

Trois vulnérabilités découvertes dans *Microsoft Sharepoint* ont été corrigées. Ces vulnérabilités permettent à un attaquant d'injecter du code JavaScript arbitraire exécuté par le navigateur de l'utilisateur *Microsoft Sharepoint*.

4 Description

Trois vulnérabilités découvertes dans *Microsoft Sharepoint* ont été corrigées. Ces vulnérabilités permettent à un attaquant d'injecter du code JavaScript arbitraire exécuté par le navigateur de l'utilisateur *Microsoft Sharepoint*.

point. L'attaquant dispose alors de la capacité d'exécuter des commandes *Microsoft Sharepoint* avec le contexte de sécurité de l'utilisateur du site.

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 MS12-011 du 14 février 2012 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-011>
<http://technet.microsoft.com/en-us/security/bulletin/MS12-011>
- Référence CVE CVE-2012-0017 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0017>
- Référence CVE CVE-2012-0144 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0144>
- Référence CVE CVE-2012-0145 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0145>

Gestion détaillée du document

15 février 2012 version initiale.