



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 septembre 2011
N° CERTA-2011-AVI-514

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-2011-AVI-514>

Gestion du document

Référence	CERTA-2011-AVI-514
Titre	Vulnérabilités dans Microsoft SharePoint
Date de la première version	14 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-074 du 13 septembre 2011
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 la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Office Groove 2007 Service Pack 2 ;
- Microsoft SharePoint Workspace 2010 (32 bits et 64 bits) ;
- Microsoft SharePoint Workspace 2010 Service Pack 1 (32 bits et 64 bits) ;
- Microsoft Office Forms Server 2007 Service Pack 2 (32 bits et 64 bits) ;
- Microsoft Office SharePoint Server 2007 Service Pack 2 (32 bits et 64 bits) ;
- Microsoft Office SharePoint Server 2010 ;
- Microsoft Office SharePoint Server 2010 Service Pack 1 ;
- Microsoft Office Groove Data Bridge Server 2007 Service Pack 2 ;
- Microsoft Office Groove Management Server 2007 Service Pack 2 ;
- Microsoft Groove Server 2010 ;
- Microsoft Groove Server 2010 Service Pack 1 ;
- Microsoft Windows SharePoint Services 2.0 ;

- Microsoft Windows SharePoint Services 3.0 Service Pack 2 (32 bits et 64 bits) ;
- Microsoft SharePoint Foundation 2010 ;
- Microsoft SharePoint Foundation 2010 Service Pack 1 ;
- Microsoft Office Web Apps 2010 ;
- Microsoft Office Web Apps 2010 Service Pack 1.

3 Résumé

Plusieurs vulnérabilités dans Microsoft SharePoint permettent à une personne malintentionnée d'élever ses privilèges sur le système.

4 Description

Plusieurs vulnérabilités dans Microsoft SharePoint ont été découvertes :

- une vulnérabilité de type injection de code indirecte permet à une personne malintentionnée de porter atteinte à la confidentialité des données ou d'élever ses privilèges sur le système vulnérable via une adresse réticulaire spécialement conçue contenant du *JavaScript* (CVE-2011-0653) ;
- une erreur dans la fonction *SafeHTML* permet d'effectuer une injection de code indirecte (CVE-2011-1252) ;
- une injection de code *JavaScript* malveillant est possible via un site Web spécialement conçu. L'exploitation de cette vulnérabilité permet une injection de code indirecte, une atteinte à la confidentialité des données et une élévation de privilèges (CVE-2011-1890) ;
- une injection de code indirecte est possible via une vulnérabilité non détaillée (CVE-2011-1891) ;
- une atteinte à la confidentialité des données est possible via un fichier *XML* spécialement conçu (CVE-2011-1892) ;
- une injection de code *JavaScript* encodé dans une adresse réticulaire spécialement conçue permet à une personne malintentionnée de porter atteinte à la confidentialité des données et d'élever ses privilèges sur le système (CVE-2011-1893).

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 MS11-074 du 13 septembre 2011 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-074>
<http://www.microsoft.com/technet/security/Bulletin/MS11-074.mspx>
- Référence CVE CVE-2011-0653 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0653>
- Référence CVE CVE-2011-1252 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1252>
- Référence CVE CVE-2011-1890 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1890>
- Référence CVE CVE-2011-1891 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1891>
- Référence CVE CVE-2011-1892 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1892>
- Référence CVE CVE-2011-1893 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1893>

Gestion détaillée du document

14 septembre 2011 version initiale.