Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2012
N° CERTA-2012-AVI-382

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft SharePoint

Gestion du document

Référence	CERTA-2012-AVI-382
Titre	Vulnérabilité dans Microsoft SharePoint
Date de la première version	11 juillet 2012
Date de la dernière version	–
Source(s)	Byulletin de sécurité Microsoft MS12-050 du 10 Juilllet 2012
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 l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Microsoft InfoPath 2007 Service Pack 2 ;
- Microsoft InfoPath 2007 Service Pack 3 ;
- Microsoft InfoPath 2010 (éditions 32 bits) ;
- Microsoft InfoPath 2010 Service Pack 1 (éditions 32 bits) ;
- Microsoft InfoPath 2010 (éditions 64 bits) ;
- Microsoft InfoPath 2010 Service Pack 1 (éditions 64 bits) ;
- Microsoft Office SharePoint Server 2007 Service Pack 2 (éditions 32 bits) ;
- Microsoft Office SharePoint Server 2007 Service Pack 3 (éditions 32 bits) ;
- Microsoft Office SharePoint Server 2007 Service Pack 2 (éditions 64 bits) ;
- Microsoft Office SharePoint Server 2007 Service Pack 3 (éditions 64 bits) ;

- Microsoft SharePoint Server 2010 ;
- Microsoft SharePoint Server 2010 Service Pack 1 ;
- Microsoft Groove Server 2010 ;
- Microsoft Groove Server 2010 Service Pack 1 ;
- Microsoft Windows SharePoint Services 3.0 Service Pack 2 (version 32 bits) ;
- Microsoft Windows SharePoint Services 3.0 Service Pack 2 (version 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 ont été corrigées dans divers produits *Microsoft*. Quatre (CVE-2012-1858, CVE-2012-1859, CVE-2012-1861, CVE-2012-1863) permettent à un utilisateur malveillant d'injecter indirectement du code à distance (XSS) dans le contexte de l'utilisateur piégé. Deux (CVE-2012-1860, CVE-2012-1862) concernent la divulgation, l'usurpation ou la modification d'informations sensibles.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS12-050 du 10 juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-050
  http://technet.microsoft.com/en-us/security/bulletin/MS12-050
- Référence CVE CVE-2012-1858 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1858
- Référence CVE CVE-2012-1859 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1859
- Référence CVE CVE-2012-1860 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1860
- Référence CVE CVE-2012-1861 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1861
- Référence CVE CVE-2012-1862 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1862
- Référence CVE CVE-2012-1863 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1863

Gestion détaillée du document

11 juillet 2012 version initiale.