

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le composant de nettoyage HTML de Microsoft

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-556>

Gestion du document

Référence	CERTA-2012-AVI-556
Titre	Vulnérabilité dans le composant de nettoyage HTML de Microsoft
Date de la première version	10 octobre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-066 du 09 octobre 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

- Élévation de privilèges
- atteinte à la confidentialité des données

2 Systèmes affectés

- Microsoft InfoPath 2007 Service Pack 2
- Microsoft InfoPath 2007 Service Pack 3
- Microsoft InfoPath 2010 Service Pack 1 éditions 32 bits
- Microsoft InfoPath 2010 Service Pack 1 éditions 64 bits
- Microsoft Communicator 2007 R2
- Microsoft Lync 2010 (32 bits)
- Microsoft Lync 2010 (64 bits)
- Microsoft Lync 2010 Attendee
- Microsoft SharePoint Server 2007 Service Pack 2 éditions 32 bits
- Microsoft SharePoint Server 2007 Service Pack 3 éditions 32 bits
- Microsoft SharePoint Server 2007 Service Pack 2 éditions 64 bits
- Microsoft SharePoint Server 2007 Service Pack 3 éditions 64 bits
- Microsoft SharePoint Server 2010 Service Pack 1

3 Résumé

Une vulnérabilité a été corrigée dans le composant de nettoyage HTML de *Microsoft*. Elle permet à un attaquant une élévation de ses privilèges en envoyant du contenu spécialement conçu.

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 MS12-066 du 09 octobre 2012 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-066>
<http://technet.microsoft.com/en-us/security/bulletin/MS12-066>
- Référence CVE CVE-2012-2520 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2520>

Gestion détaillée du document

10 octobre 2012 version initiale.