



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2012
N° CERTA-2012-AVI-554

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Office

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-554>

Gestion du document

Référence	CERTA-2012-AVI-554
Titre	Vulnérabilités dans Microsoft Office
Date de la première version	10 octobre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 10 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Office 2003 Service Pack 3
- Microsoft Office 2007 Service Pack 2
- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 1 (édition 32-bit)
- Microsoft Office 2010 Service Pack 1 (édition 64-bit)
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack Service Pack 2
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft SharePoint Server 2010 Service Pack 1
- Microsoft Office Web Apps 2010 Service Pack 1

3 Résumé

Deux vulnérabilités ont été corrigées dans *Microsoft Office*. Une concerne une exécution de code arbitraire au moyen d'un document *Word* ayant la section PAPX spécialement conçue. La seconde permet également une exécution de code arbitraire à distance au moyen d'une utilisation de données après libération (use-after-free) présente dans le format RTF.

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 MS12-064 du 09 octobre 2012 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-064>
<http://technet.microsoft.com/en-us/security/bulletin/MS12-064>
- Référence CVE CVE-2012-0182 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0182>
- Référence CVE CVE-2012-2528 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2528>

Gestion détaillée du document

10 octobre 2012 version initiale.