

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Office Publisher 2007

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-2007-AVI-292>

Gestion du document

Référence	CERTA-2007-AVI-292
Titre	Vulnérabilité de Microsoft Office Publisher 2007
Date de la première version	11 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-037 du 10 juillet 2007
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

– Vulnérabilité de Microsoft Office Publisher 2007 dans la suite bureautique Microsoft Office 2007.

Les versions précédentes de l'application ne seraient pas affectées par cette vulnérabilité.

3 Description

Une vulnérabilité a été identifiée dans l'application Publisher 2007, un composant disponible avec la suite bureautique Microsoft Office 2007.

Cette dernière n'effacerait pas de manière satisfaisante les ressources en mémoire, au cours de l'opération d'écriture de données entre le disque et la mémoire. Plus précisément, l'erreur proviendrait de la bibliothèque de conversion PUBCONV.DLL utilisée par Publisher pour « convertir » des documents produits par des versions antérieures de Publisher.

Une personne malveillante pourrait donc construire une page .pub particulière, exploitant cette vulnérabilité. A l'ouverture de cette page sur un système vulnérable, du code arbitraire pourrait être exécuter à l'insu de l'utilisateur.

4 Solution

Se référer au bulletin de sécurité MS07-037 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS07-037 du 10 juillet 2007 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-037.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-037.msp>
- Référence CVE CVE-2007-1754 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1754>

Gestion détaillée du document

11 juillet 2007 version initiale.