

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Office Publisher

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-2008-AVI-075>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2008-AVI-075 |
| Titre | Vulnérabilités dans Microsoft Office Publisher |
| Date de la première version | 13 février 2008 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS08-012 du 12 février 2008 |
| 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 Publisher 2000 dans Microsoft Office 2000 Service Pack 3 ;
- Microsoft Office Publisher 2002 dans Microsoft Office XP Service Pack 3 ;
- Microsoft Office Publisher 2003 SP2 dans Microsoft Office 2003 Service Pack 2.

3 Résumé

Des vulnérabilités ont été identifiées dans l'application Microsoft Office Publisher. L'exploitation de ces dernières peut entraîner dans certaines conditions l'exécution de code arbitraire sur le système vulnérable.

4 Description

Des vulnérabilités ont été identifiées dans l'application Microsoft Office Publisher. Parmi celles-ci :
– les données de l'application ne seraient pas correctement vérifiées lors du chargement de fichiers Publisher

- en mémoire. Une personne pourrait exploiter cette vulnérabilité au moyen d'un fichier .pub spécialement construit afin d'exécuter des commandes malveillantes sur le système lors de son ouverture ;
- les valeurs d'index mémoire ne seraient pas correctement validées. Une personne pourrait également exploiter cette vulnérabilité au moyen d'un fichier .pub spécialement construit.

5 Solution

Se référer au bulletin de sécurité MS08-012 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-012 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-012.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-012.msp>
- Référence CVE CVE-2008-0102 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0102>
- Référence CVE CVE-2008-0104 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0104>

Gestion détaillée du document

13 février 2008 version initiale.