Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 avril 2008
N° CERTA-2008-AVI-190

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Office Viso

Gestion du document

Référence	CERTA-2008-AVI-190
Titre	Vulnérabilités dans Microsoft Office Viso
Date de la première version	09 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-019 du 08 avril 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

- Visio 2002 Service Pack 2 dans Microsoft Office XP Service Pack 2 ;
- Visio 2003 Service Pack 2 dans Microsoft Office 2003 Service Pack 2 ;
- Visio 2003 Service Pack 3 dans Microsoft Office 2003 Service Pack 3 ;
- Visio 2007 dans Microsoft Office System 2007 ;
- Visio 2007 Service Pack 1 dans Microsoft Office System 2007 Service Pack 1 .

Les visualiseurs (*viewer*) Visio ne seraient pas affectés.

3 Résumé

Deux vulnérabilités ont été identifiées dans l'application bureautique Microsoft Visio. L'exploitation de ces vulnérabilités par le biais d'un fichier spécialement construit permettrait d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Deux vulnérabilités ont été identifiées dans l'application bureautique Microsoft Visio destinée à la création de diagrammes et de synoptiques.

- l'application ne validerait pas correctement les données d'en-tête des objets dans les fichiers ;
- l'application ne validerait pas correctement les allocations de mémoire lors du chargement des fichiers au format `.DFX`. Il s'agit du format de fichiers de dessin AutoCAD qui n'est pas associé à Microsoft Viso par défaut.

L'exploitation de ces vulnérabilités peut se faire par le biais d'un fichier spécialement construit. Si celui-ci est ouvert sur un système vulnérable, il pourrait alors provoquer l'exécution de commandes arbitraires.

5 Solution

Se référer au bulletin de sécurité MS08-019 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-019 du 08 avril 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-019.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-019.mspx
- Référence CVE CVE-2008-1089 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1089
- Référence CVE CVE-2008-1090 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1090

Gestion détaillée du document

09 avril 2008 version initiale.