



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 février 2009  
N° CERTA-2009-AVI-062

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Microsoft Visio

---

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-2009-AVI-062>

---

### Gestion du document

Référence	CERTA-2009-AVI-062
Titre	Multiples vulnérabilités dans Microsoft Visio
Date de la première version	11 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-005 du 10 février 2009
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 Visio 2002 Service Pack 2 et les versions antérieures ;
- Microsoft Visio 2003 Service Pack 3 et les versions antérieures ;
- Microsoft Visio 2007 Service Pack 1 et les versions antérieures.

## 3 Résumé

Plusieurs vulnérabilités affectant *Microsoft Visio* permettent à un individu malveillant d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités sont présentes dans *Microsoft Visio* :

- la première (CVE-2009-0095) concerne la validation des objets d'un document *Visio* lors de son ouverture,

un individu malveillant peut exécuter du code arbitraire à distance par le biais d'un fichier spécialement fabriqué ;

- la seconde (CVE-2009-0096 et CVE-2009-0097) concerne la gestion et le stockage des objets *Visio* dans la mémoire, un individu malveillant peut exécuter du code arbitraire à distance par le biais d'un fichier spécialement fabriqué.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS09-005 du 10 février 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-005.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-005.msp>
- Référence CVE CVE-2009-0095 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0095>
- Référence CVE CVE-2009-0096 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0096>
- Référence CVE CVE-2009-0097 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0097>

## Gestion détaillée du document

11 février 2009 version initiale.