



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 novembre 2006
N° CERTA-2006-AVI-479

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Visual Studio

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-2006-AVI-479>

Gestion du document

Référence	CERTA-2006-AVI-479
Titre	Vulnérabilité dans Microsoft Visual Studio
Date de la première version	07 novembre 2006
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft du 31 octobre 2006
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 Visual Studio 2005.

3 Résumé

Une vulnérabilité dans Microsoft Visual Studio permet à une personne distante malintentionnée d'exécuter du code arbitraire.

4 Description

Une vulnérabilité présente dans un contrôle ActiveX dans Microsoft Visual Studio permet à un utilisateur distant malintentionné d'exécuter du code arbitraire.

Le contrôle ActiveX concerné est `WMI Object Broker` inclus dans `WmiScriptUtils.dll`.

5 Contournement provisoire

Microsoft propose plusieurs solutions de contournement dans son bulletin de sécurité, dont le blocage de l'exécution de l'ActiveX dans Internet Explorer en définissant le Kill bit relatif au contrôle dans le registre.

6 Solution

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

7 Documentation

- Bulletin de sécurité Microsoft 927709 du 31 octobre 2006 :
<http://www.microsoft.com/france/technet/security/advisory/927709.msp>
<http://www.microsoft.com/technet/security/advisory/927709.msp>
- Référence CVE CVE-2006-4704 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4704>

Gestion détaillée du document

07 novembre 2006 version initiale.