

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Active Template Library ActiveX controls pour Microsoft Office

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-440>

Gestion du document

Référence	CERTA-2009-AVI-440
Titre	Multiples vulnérabilités dans Microsoft ATL ActiveX controls pour Microsoft Office
Date de la première version	14 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-060 du 13 octobre 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2003 Service Pack 3 ;
- 2007 Microsoft Office System Service Pack 1 et 2 ;
- Microsoft Visio 2002 Viewer ;
- Microsoft Office Visio 2003 Viewer ;
- Microsoft Office Vision Viewer Service Pack 2 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans Microsoft Active Template Library (ATL) ActiveX controls pour Microsoft Office permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités dans Microsoft Active Template Library (ATL) ActiveX controls pour Microsoft Office permettent à une personne distante d'exécuter du code arbitraire :

- une erreur dans l'en-tête de Microsoft ATL permet d'exécuter du code arbitraire à distance via l'appel *VariantClear* (CVE-2009-0901);
- une erreur dans l'en-tête de Microsoft ATL permet d'exécuter du code arbitraire à distance via l'instanciation d'un objet issu d'un flux de données (CVE-2009-2493);
- une erreur dans Microsoft ATL permet de lire une chaîne de caractères sans le caractère *NULL* de fin. Il est ainsi possible de lire des données supplémentaires présentes en mémoire.

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 MS09-060 du 13 octobre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-060.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS09-060.mspx>
- Référence CVE CVE-2009-0901 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0901>
- Référence CVE CVE-2009-2493 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493>
- Référence CVE CVE-2009-2495 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2495>

Gestion détaillée du document

14 octobre 2009 version initiale.