Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juin 2011
N° CERTA-2011-AVI-346

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft OLE Automation

Gestion du document

Référence	CERTA-2011-AVI-346
Titre	Vulnérabilité dans Microsoft OLE Automation
Date de la première version	15 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS11-038 du 14 juin 2011
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

- Windows XP Service Pack 3 ;
- Windows XP Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 bits et Windows 7 pour systèmes 32 bits Service Pack 1 ;
- Windows 7 pour systèmes x64 et Windows 7 pour systèmes x64 Service Pack 1 ;

- Windows Server 2008 R2 pour systèmes x64 et Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium et Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

3 Résumé

Une vulnérabilité dans Microsoft Windows OLE (*Object Linking and Embedding*) Automation permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité dans Microsoft Windows OLE Automation permet à une personne malintentionnée d'exécuter de code à distance à distance via une page Web contenant une image WMF (*Windows Metafile*) spécialement conçue.

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 MS11-038 du 14 juin 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-038.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-038.mspx
- Référence CVE CVE-2011-0658 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0658

Gestion détaillée du document

15 juin 2011 version initiale.