



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 janvier 2012
N° CERTA-2012-AVI-011

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Windows

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-2012-AVI-011>

Gestion du document

Référence	CERTA-2012-AVI-011
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	11 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS12-005 du 10 janvier 2012
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 Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 with SP2 for Itanium-based Systems ;
- Windows Vista Service Pack2 ;
- Windows Vista x64 Edition Service Pack2 ;
- Windows Server 2008 for 32-bit Systems Service Pack 2 ;
- Windows Server 2008 for x64-based Systems Service Pack 2 ;
- Windows Server 2008 for Itanium-based Systems Service Pack 2 ;
- Windows 7 for 32-bit Systems et Windows 7 for 32-bit Systems Service Pack 1 ;
- Windows 7 for x64-based Systems et Windows 7 for x64-based Systems Service Pack 1 ;

- Windows Server 2008 R2 for x64-based Systems et Windows Server 2008 R2 for x64-based Systems Service Pack 1 ;
- Windows Server 2008 R2 for Itanium-based Systems et Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 ;

3 Résumé

Une vulnérabilité permettant à une personne malintentionnée d'exécuter du code arbitraire à distance est présente dans *Microsoft Windows*.

4 Description

Une vulnérabilité non spécifiée permet à un utilisateur distant malintentionné d'exécuter du code arbitraire lors de l'ouverture d'un document *Microsoft Office* contenant une application *ClickOnce* spécialement conçue. Cette vulnérabilité a été classifiée comme *importante* par l'éditeur.

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 MS12-005 du 10 janvier 2012 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-005>
<http://technet.microsoft.com/en-us/security/bulletin/MS12-005>
- Référence CVE CVE-2012-0013 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0013>

Gestion détaillée du document

11 janvier 2012 version initiale.