



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 septembre 2006
N° CERTA-2006-AVI-410

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du système 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-2006-AVI-410>

Gestion du document

Référence	CERTA-2006-AVI-410
Titre	Vulnérabilité du système Microsoft Windows
Date de la première version	27 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS06-055 de Microsoft du 26 septembre 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 Windows XP Service Pack 1 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows 2003 pour Itanium ;
- Microsoft Windows Server 2003 Service Pack 1 et Microsoft Windows 2003 pour Itanium Service Pack 1 ;
- Microsoft Windows Server 2003 x64.

3 Résumé

Une vulnérabilité permettant d'exécuter du code arbitraire à distance a été découverte dans la bibliothèque Windows de gestion des images vectorielles (vgx.dll).

4 Description

Une vulnérabilité a été découverte dans la bibliothèque de gestion des documents au format VML (*Vector Markup Language*). Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur une machine distante vulnérable par l'intermédiaire d'un document VML spécialement construit.

Cette vulnérabilité a fait l'objet d'une alerte par le CERTA le 31 août 2006 (cf. CERTA-2006-ALE-011).

Des codes d'exploitation, utilisés dans certains cas dans des logiciels malveillants, circulent actuellement sur l'Internet.

5 Contournement provisoire

Se référer à l'alerte du CERTA référencé sous le numéro CERTA-2006-ALE-011

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 MS06-055 du 26 septembre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-055.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-055.msp>
- Alerte du CERTA numéro CERTA-2006-ALE-011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-011/index.html>
- Référence CVE CVE-2006-4868 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4868>

Gestion détaillée du document

27 septembre 2006 version initiale.