Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 janvier 2010
N° CERTA-2010-AVI-011

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Windows

Gestion du document

Référence	CERTA-2010-AVI-011
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	13 janvier 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-001 du 12 janvier 2010
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 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et Windows XP Service Pack 3 ;
- Microsoft Windows XP Professionnel Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Microsoft Windows Vista, Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Microsoft Windows Vista Édition x64, Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;

- Microsoft Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Microsoft Windows 7 pour systèmes 32 bits ;
- Microsoft Windows 7 pour systèmes x64 ;
- Microsoft Windows Server 2008 R2 pour systèmes x64 ;
- Microsoft Windows Server 2008 R2 pour systèmes Itanium.

3 Résumé

Une vulnérabilité dans `Microsoft Windows` permet à un utilisateur distant malintentionné d'exécuter du code arbitraire.

4 Description

La technologie `Embedded OpenType` (`EOT`) permet d'inclure des polices de caractères (*fonts*) dans divers documents comme des pages en `HTML` ou des documents `Microsoft Office`. Une vulnérabilité relative à la mise en œuvre de cette technologie est présente dans `Microsoft Windows` et permet à un utilisateur distant malintentionné d'exécuter du code arbitraire.

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 MS10-001 du 12 janvier 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-001.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-001.mspx

Gestion détaillée du document

13 janvier 2010 version initiale.