



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 décembre 2008
N° CERTA-2008-AVI-585

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la bibliothèque GDI de 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-2008-AVI-585>

Gestion du document

Référence	CERTA-2008-AVI-585
Titre	Multiples vulnérabilités dans la bibliothèque GDI de Microsoft Windows
Date de la première version	09 décembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-071 du 09 décembre 2008
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 ;
- Windows XP Service Pack 2 ;
- Windows XP Service Pack 3 ;
- Windows XP Professionnel Édition x64 ;
- Windows XP Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 1 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP1 pour systèmes Itanium ;
- Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Windows Vista et Windows Vista Service Pack 1 ;
- Windows Vista Édition x64 ;

- Windows Vista Édition x64 Service Pack 1 ;
- Windows Server 2008 pour systèmes 32 bits ;
- Windows Server 2008 pour systèmes x64 ;
- Windows Server 2008 pour systèmes Itanium.

3 Résumé

Plusieurs vulnérabilités dans la bibliothèque *GDI (Graphics Device Interface)* de Microsoft Windows permettent à une personne distante d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités dans la bibliothèque *GDI* de Microsoft Windows permettent à une personne distante d'exécuter du code arbitraire :

- une erreur liée au mode de traitement des calculs d'entiers permet d'exécuter du code arbitraire à distance via un fichier image *WMF* spécialement conçu ;
- une erreur dans le traitement des paramètres de taille de fichier dans les fichiers *WMF* permet d'exécuter du code arbitraire à distance.

5 Solution

Se référer au bulletin de sécurité MS08-071 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-071 du 09 décembre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-071.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-071.msp>
- Référence CVE CVE-2008-2249 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2249>
- Référence CVE CVE-2008-3465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3465>

Gestion détaillée du document

09 décembre 2008 version initiale.