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 novembre 2005
N° CERTA-2005-AVI-445-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le moteur de rendu graphique de Microsoft

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-445

Gestion du document

Référence	CERTA-2005-AVI-445-001
Titre	Multiples vulnérabilités dans le moteur de rendu graphique de Microsoft
Date de la première version	09 novembre 2005
Date de la dernière version	09 novembre 2005
Source(s)	Bulletin de sécurité Microsoft MS05-053 du 08 novembre 2005
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 ;
- déni de service.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP Professional 64-Bit Edition ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour systèmes Itanium ;
- Microsoft Windows Server 2003 Service Pack 1 pour systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition ;
- produits Avaya utilisant Microsoft Windows : Unified Communication Center, Modular Messaging - Messaging Application Server et S8100/DefinityOne/IP600 Media Servers.

3 Résumé

Plusieurs vulnérabilités découvertes dans le moteur de rendu graphique de Microsoft permettent à un utilisateur mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Le moteur de rendu graphique de Microsoft permet le traitement de fichiers au format `WMF` (Windows MetaFile) et `EMF` (Enhanced MetaFile).

- Une vulnérabilité de type débordement de mémoire peut être exploitée au moyen d'une image `WMF` ou `EMF` malicieusement contruite afin d'exécuter du code arbitraire à distance via un site web ou un message électronique malveillants (CAN-2005-2123) ;
- une seconde vulnérabilité de type débordement de mémoire peut être exploitée au moyen d'une image `WMF` malicieusement construite afin d'exécuter du code arbitraire à distance (CAN-2005-2124) ;
- une vulnérabilité de type débordement de mémoire permet de provoquer un déni de service au moyen d'une image `EMF` malicieusement construite. Cette vulnérabilité ne permet pas l'exécution de code arbitraire (CAN-2005-0803).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de l'éditeur :
  http://www.microsoft.com/france/
- Bulletin de sécurité Microsoft MS05-053 du 08 novembre 2005 :
  http://www.microsoft.com/france/technet/securite/ms05-053.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx
- Bulletin de sécurité Avaya ASA-2005-228 du 08 novembre 2005 :
  http://support.avaya.com/elmodocs2/security/ASA-2005-228.pdf
- Référence CVE CAN-2005-0803 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0803
- Référence CVE CAN-2005-2123 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2123
- Référence CVE CAN-2005-2124 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2124

Gestion détaillée du document

09 novembre 2005 version initiale ;
09 novembre 2005 ajout du bulletin de sécurité Avaya.