Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 juin 2006
N° CERTA-2006-ALE-006-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Word

Gestion du document

Référence	CERTA-2006-ALE-006-001
Titre	Vulnérabilité dans Microsoft Word
Date de la première version	20 mai 2006
Date de la dernière version	14 juin 2006
Source(s)	Bulletin du SANS du 19 mai 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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Word 2003 ;
- Microsoft Word 2002 ;
- Microsoft Word 2000.

3 Résumé

Une vulnérabilité non corrigée dans Microsoft Word permettrait à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.

4 Description

Une vulnérabilité de nature pour le moment inconnue dans Microsoft Word permettrait à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance sur les versions 2002 et 2003 de Microsoft Word ou de provoquer un déni de service sur la version 2000. Cette vulnérabilité fait l'objet d'une utilisation par du code malveillant sur l'Internet. Elle est exploitable par le biais d'un fichier `doc` construit de façon particulière.

5 Contournement provisoire

5.1 Utiliser un logiciel alternatif

Il semblerait que le visualiseur de documents Word de Microsoft ne soit pas affecté par cette vulnérabilité. Il est donc possible de l'utiliser pour une simple consultation. Cependant il convient plutôt d'utiliser un traitement de texte alternatif comme `Abiword` ou celui de `OpenOffice.org`.

5.2 Mettre à jour la base de signatures d'antivirus

Certains éditeurs d'antivirus proposent déjà des mises à jours de signatures prenant en compte le code malveillant sous sa forme actuelle. Il est cependant probable que des variantes apparaissent afin de contourner ces antivirus.

5.3 N'ouvrir que les documents provenant de sources de confiance

A la reception d'un document au format `doc` soit par le biais de la messagerie électronique ou sur tout autre support, il est nécessaire de s'assurer de la provenance de ce fichier et de ne l'ouvrir que si la source est de confiance.

6 Solution

Appliquer le correctif de l'éditeur (Cf. section documentation)

7 Documentation

- Bulletin de sécurité de Microsoft du 13 juin 2006:
  http://www.microsoft.com/technet/security/Bulletin/MS06-027.mspx
- Bulletin du SANS du 19 mai 2006 :
  http://isc.sans.org/diary.php/storyid=1347
- Site du Microsoft Security Response Center :
  http://blogs.technet.com/msrc/
- Bulletin de sécurité de l'US-CERT du 19 mai 2006 :
  http://www.us-cert.gov/cas/alerts/SA06-139A.html

Gestion détaillée du document

20 mai 2006 version initiale.
14 juin 2006 ajout du correctif de Microsoft