



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 décembre 2004  
N° CERTA-2004-AVI-392

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans WordPad

---

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-2004-AVI-392>

---

### Gestion du document

Référence	CERTA-2004-AVI-392
Titre	Vulnérabilités dans WordPad
Date de la première version	15 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Microsoft MS04-041 du 14 décembre 2004
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

- Windows NT Server 4.0 Service Pack 6a ;
- Windows NT Server 4.0 Terminal Server Edition Service Pack 6 ;
- Windows 2000 Service Pack 3 et 4 ;
- Windows XP Service Pack 1 et 2 ;
- Windows XP 64-Bit Edition Service Pack 1 ;
- Windows XP 64-Bit Edition Version 2003 ;
- Windows Server 2003 ;
- Windows Server 2003 64-Bit Edition.

## 3 Résumé

Deux vulnérabilités dans le convertisseur de format Word 6.0 en format WordPad permettent l'exécution de code arbitraire à distance.

## 4 Description

L'utilitaire WordPad permet de lire et de modifier le contenu de certains types de fichiers, notamment ceux ayant pour extension `.wri`, `.doc` ou `.rtf`. Deux vulnérabilités dans le convertisseur de format Word 6.0 en format WordPad permettent à un utilisateur mal intentionné, par le biais d'un fichier ou d'un site web malicieusement constitués, d'exécuter du code arbitraire à distance.

## 5 Solution

Appliquer le correctif de Microsoft, en fonction de votre système d'exploitation, tel qu'indiqué dans le bulletin de sécurité MS04-041 (voir Documentation).

## 6 Documentation

- Bulletin de sécurité de Microsoft MS04-041 du 14 décembre 2004 :  
<http://www.microsoft.com/technet/security/bulletin/MS04-041.msp>
- Référence CVE CAN-2004-0571 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0571>
- Référence CVE CAN-2004-0901 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0901>

## Gestion détaillée du document

15 décembre 2004 version initiale.