

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans 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-2009-AVI-142>

---

### Gestion du document

Référence	CERTA-2009-AVI-142
Titre	Vulnérabilités dans Microsoft Windows
Date de la première version	15 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-012 du 14 avril 2009
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et 3 ;
- Microsoft Windows XP Professional Edition pour systèmes x64, Service Pack 2 compris ;
- Microsoft Windows Server 2003 Service Pack 1 et 2, y compris pour les systèmes x64 et Itanium ;
- Microsoft Windows Vista, Service Pack 1 inclus, y compris pour les versions x64 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits, x64 et Itanium.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Microsoft Windows. Leur exploitation peut conduire à une élévation de privilèges.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Microsoft Windows. Elles concernent :

- le service de transaction MSDTC (*Microsoft Distributed Transaction Coordinator*) qui permet d'obtenir certains jetons (NetworkService) lors d'appels RPC ;
- le service de gestion WMI (*Windows Management Instrumentation*) qui permet de récupérer sous certaines conditions les privilèges au niveau LocalSYSTEM ;
- le service serveur RPC (RPCSS) qui permet de récupérer sous certaines conditions les droits LocalSYSTEM ;
- la classe ThreadPool de Windows qui permet également d'exécuter, selon le positionnement des listes de contrôles d'accès des threads, du code avec des droits élevés LocalSYSTEM.

Certaines de ces vulnérabilités ont fait l'objet de l'alerte CERTA-2008-ALE-012 publiée le 10 octobre 2008.

## 5 Solution

Se référer au bulletin de sécurité MS09-012 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS09-012 du 14 avril 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-012.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-012.msp>
- Référence CVE CVE-2008-1436 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1436>
- Référence CVE CVE-2009-0078 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0078>
- Référence CVE CVE-2009-0079 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0079>
- Référence CVE CVE-2009-0080 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0080>
- Alerte du CERTA CERTA-2008-ALE-012 du 10 octobre 2008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-012/>

## Gestion détaillée du document

15 avril 2009 version initiale.