

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans « Service Control Manager » de Windows 2000

---

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-2000-AVI-023>

---

### Gestion du document

Référence	CERTA-2000-AVI-023
Titre	Vulnérabilité dans le « Service Control Manager » de Windows 2000
Date de la première version	07 août 2000
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Microsoft Avis du CERT IST
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, modification et usurpation de privilèges en local.

## 2 Systèmes affectés

Windows 2000.

## 3 Résumé

Service control Manager (SMC) est un outil de Windows 2000 permettant d'administrer les services de la machine : création, modification, etc.

Une vulnérabilité liée à la façon dont est gérée l'initialisation d'un service y a été découverte.

## 4 Description

Lors de la préparation de l'environnement de démarrage d'un service, sous Windows 2000, le SMC utilise une mémoire « *pipe* » à laquelle elle donne un nom pour permettre le dialogue entre deux processus parents. Le nom de cette mémoire « *pipe* » est prévisible.

Un utilisateur local mal intentionné peut alors créer cette zone mémoire avant l'initialisation du SMC, voire même, de l'allouer à un processus malicieux, ce qui lui permettrait d'interagir avec le service dans son contexte, et d'obtenir ainsi des privilèges auxquels il n'a pas le droit, même ceux de l'administrateur de la machine.

## 5 Solution

Appliquer le correctif ci dessous :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23432>

## 6 Documentation

- Le bulletin de sécurité Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/ms00-053.asp>
- La FAQ de Microsoft au sujet de ce bulletin :  
<http://www.microsoft.com/technet/security/bulletin/fq00-053.asp>
- L'article de la base de connaissance concernant ce bulletin :  
<http://www.microsoft.com/technet/support/kb.asp?269523>

## Gestion détaillée du document

07 août 2000 version initiale.