

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans MS-SQL Server

---

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-2003-AVI-117>

---

### Gestion du document

Référence	CERTA-2003-AVI-117
Titre	Vulnérabilités dans MS-SQL Server
Date de la première version	24 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS03-031 de Microsoft
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 ;
- élévation de privilèges ;
- déni de service.

## 2 Systèmes affectés

- Microsoft SQL Server 7.0 ;
- Microsoft Data Engine (MSDE) 1.0 ;
- Microsoft SQL Server 2000 ;
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) ;
- Microsoft SQL Server 2000 Desktop Engine (Windows).

## 3 Résumé

Trois vulnérabilités ont été découvertes dans MS SQL Server.

## 4 Description

- Microsoft SQL Server utilise des tubes nommés spécifiques pour la gestion des connexions au serveur. Une erreur dans le mécanisme de gestion utilisé pour ces tubes permet à un utilisateur local non autorisé d'obtenir un accès au serveur en prenant possession d'un tube nommé utilisé pour la connexion d'un utilisateur licite ;
- l'envoi d'un paquet malicieusement formé à un tube nommé spécifique permet à un utilisateur mal intentionné d'effectuer un déni de service ou bien d'exécuter du code arbitraire sur le serveur ;
- une faille de type débordement de mémoire présente dans l'une des fonctions du serveur permet à un utilisateur local d'exécuter du code arbitraire sur la machine.

## 5 Solution

Appliquer le correctif cumulatif fourni par Microsoft (cf. Documentation).

## 6 Documentation

Bulletin de sécurité #MS03-031 de Microsoft :

<http://www.microsoft.com/technet/security/MS03-031.asp>

Référence CVE CAN-2003-0230 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0230>

Référence CVE CAN-2003-0231 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0231>

Référence CVE CAN-2003-0232 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0232>

## Gestion détaillée du document

24 juillet 2003 version initiale.