

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Microsoft 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-2002-AVI-082>

---

### Gestion du document

Référence	CERTA-2002-AVI-082
Titre	Vulnérabilité dans Microsoft SQL Server
Date de la première version	18 avril 2002
Date de la dernière version	–
Source(s)	Bulletin de securite MS02-020 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

- Elévation de privilèges ;
- exécution de code arbitraire ;
- Déni de service.

## 2 Systèmes affectés

- Microsoft SQL Server 7.0 ;
- Microsoft SQL Server 2000.

## 3 Résumé

Des vulnérabilités ont été découvertes dans certaines procédures stockées étendues du serveur SQL de Microsoft.

## **4 Description**

Une procédure stockée étendue est une procédure stockée qui exécute du code écrit en langage de programmation et non des commandes de base de données. Certaines des procédures stockées étendues fournies dans SQL Server contiennent des vulnérabilités de type débordement de mémoire. Un utilisateur mal intentionné peut exploiter ces vulnérabilités afin d'exécuter du code arbitraire avec les privilèges du service MSSQL ou bien effectuer un déni de service.

## **5 Solution**

Appliquer le correctif fourni par Microsoft (cf. Documentation)

## **6 Documentation**

Bulletin de sécurité MS02-020 de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/MS02-020.asp>

## **Gestion détaillée du document**

**18 avril 2002** version initiale.