



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 25 juillet 2002  
N° CERTA-2002-AVI-156

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans MS SQL Server 2000 et MSDE 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-2002-AVI-156>

---

### Gestion du document

Référence	CERTA-2002-AVI-156
Titre	Vulnérabilités dans MS SQL Server 2000 et MSDE 2000
Date de la première version	25 juillet 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS02-038 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 à distance ;
- prise de contrôle de la base SQL.

## 2 Systèmes affectés

- MS SQL Server 2000 ;
- MSDE 2000.

## 3 Résumé

Deux vulnérabilités ont été découvertes dans MS SQL Server 2000 et MSDE 2000.

## **4 Description**

- Database Consistency Checkers (DBCCs) est un ensemble d'utilitaires exécutables en ligne de commande intégrés à SQL Server 2000 permettant d'assurer la maintenance ou d'effectuer diverses opérations sur un serveur SQL Server. Une vulnérabilité de type débordement de mémoire présente dans DBCCs permet à un individu mal intentionné d'exécuter du code arbitraire à distance dans le contexte d'exécution du service SQL Server ou bien de prendre le contrôle de la base de données.
- Une vulnérabilité d'injection SQL présente dans deux procédures stockées, utilisées pour la réplication des bases de données permet, dans certains cas, à un individu mal intentionné d'exécuter du code arbitraire à distance.

## **5 Solution**

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

## **6 Documentation**

Bulletin de sécurité Microsoft #MS02-038 :  
<http://www.microsoft.com/technet/security/bulletin/MS02-038.asp>

## **Gestion détaillée du document**

**25 juillet 2002** version initiale.