

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans MS-SQL

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-220>

Gestion du document

Référence	CERTA-2002-AVI-220
Titre	Multiples vulnérabilités dans MS-SQL
Date de la première version	03 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin de securite #MS02-056 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

- Déni de service ;
- exécution de code arbitraire ;
- élévation de privilèges ;
- prise de contrôle de la base SQL.

2 Systèmes affectés

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

3 Résumé

Trois nouvelles vulnérabilités ont été découvertes dans SQL Server.

4 Description

- Un débordement de mémoire présent dans une partie du code de SQL Server 2000 (et MSDE 2000) associé à l'authentification des utilisateurs permet d'exécuter du code arbitraire dans le contexte de sécurité du service SQL Server ou bien d'effectuer un déni de service ;
- un débordement de mémoire présent dans l'une des Database Console Commands (DBCCs) permet d'exécuter du code arbitraire avec le contexte de sécurité du service SQL Server et de prendre le contrôle des bases de données du serveur ;
- une vulnérabilité associée à la planification des tâches dans les serveurs SQL 7.0 et 2000 permet à un utilisateur mal intentionné de créer un fichier de commandes exécutable par un utilisateur lors du démarrage de son profil ou bien de remplacer certains fichiers du système afin d'en perturber le fonctionnement.

5 Solution

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

6 Documentation

Bulletin de sécurité MS02-056 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/ms02-056.asp>

Gestion détaillée du document

03 octobre 2002 version initiale.