Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 août 2002
N° CERTA-2002-AVI-177

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft SQL Server

Gestion du document

Référence	CERTA-2002-AVI-177
Titre	Vulnérabilités dans Microsoft SQL Server
Date de la première version	19 août 2002
Date de la dernière version	–
Source(s)	Avis #MS02-043 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.

2 Systèmes affectés

- Microsoft SQL Server 7.0 (incluant MSDE 1.0) ;
- Microsoft SQL Server 2000 (incluant MSDE 2000).

3 Résumé

Des vulnérabilités présentes dans les procédures étendues (extended stored procedures) permettent une élévation de privilèges.

4 Description

Les serveurs SQL de Microsoft installent par défaut des procédures étendues (extended stored procedures) qui fournissent des services spécifiques aux utilisateurs de la base de données.

Trois procédures ont une vulnérabilité commune permettant à un utilisateur mal intentionné d'élever ses privilèges vers ceux de l'application SQL Server (par défaut, les privilèges d'un utilisateur du domaine).

5 Contournement provisoire

L'étendue de la vulnérabilité dépend en grande partie de la configuration du serveur. Les règles suivantes permettent de minimiser les risques :

- Le service SQL doit, de préférence, fonctionner avec les droits d'un utilisateur du domaine auquel appartient le serveur. Les actions de l'attaquant seront alors réduites aux droits de cet utilisateur ;
- seuls les utilisateurs de confiance peuvent avoir un accès à toutes les fonctions du serveur ;
- les requêtes publiques doivent être filtrées avant tout traitement.

6 Solution

Appliquer le correctif disponible en téléchargement depuis la page web de l'avis #MS02-043 de Microsoft (consultez la section Documentation).

Ce correctif est cumulatif et inclut les corrections documentées dans les avis `CERTA-2002-AVI-082` et `CERTA-2002-AVI-156`.

Les autres vulnérabilités ne sont pas corrigées par ce correctif.

7 Documentation

Avis #MS02-043 de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS02-043.asp

Gestion détaillée du document

19 août 2002 version initiale.