Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juin 2001
N° CERTA-2001-AVI-063

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2001-AVI-063

Gestion du document

Référence	CERTA-2001-AVI-063
Titre	Vulnérabilité de MS SQL Server
Date de la première version	13 juin 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

Compromission de base de données et exécutions de commandes avec les privilèges de l'administrateur de la base.

2 Systèmes affectés

- Microsoft SQL serveur 7.0
- Microsoft SQL server 2000 Gold

3 Résumé

Des données de la session administrateur persistantes peuvent être réutilisée par un utilisateur mal intentionné.

4 Description

Pour des raisons de performances, après la déconnexion de la session de l'administrateur, certaines données restent dans le cache. Un utilisateur authentifié, ayant le droit d'accéder à la base de donnée, peut, par le biais d'une requête SQL habilement conçue, réutiliser ces données pour exécuter des commandes dans le contexte de sécurité de l'administrateur de la base.

5 Contournement provisoire

Cette vulnérabilité ne pouvant se produire qu'en *Mode Mixte*, Microsoft recommande de configurer le serveur en *Mode Authentifié*.

6 Solution

Appliquer le correctif Microsoft :
http://support.microsoft.com/support/kb/articles/Q299/7/17.asp

7 Documentation

http://www.microsoft.com/technet/security/bulletin/ms01-032.asp

Gestion détaillée du document

13 juin 2001 version initiale.