

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft SQL Serveur

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-2000-AVI-013>

Gestion du document

Référence	CERTA-2000-AVI-013
Titre	Vulnérabilité dans Microsoft SQL Serveur
Date de la première version	11 juillet 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft Sites web Security Bugware et SecurityFocus
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

Exécution de commandes non-autorisées.

2 Systèmes affectés

Toute machine utilisant Microsoft SQL Server 7.0.

3 Résumé

Une « procédure cataloguée » (ou procédure mémorisée) est un ensemble d'instructions SQL précompilées enregistré dans le dictionnaire d'une base de données SQL sur un serveur. Elles sont exécutées par une application via un appel de procédure (*Remote Procedure Call*).

Une vulnérabilité de Microsoft SQL server 7.0 permet à un utilisateur mal intentionné d'exécuter des « procédures cataloguées » auxquelles il n'a normalement pas accès.

4 Description

Dans une base de donnée SQL, tout membre du groupe Sysadmin de la base de données, est un utilisateur particulier appelé Opérateur de Base de Données (*DBO : Database Operator*).

Lorsqu'une procédure cataloguée temporaire appelle une procédure cataloguée dont le propriétaire est DBO, la vérification des permissions qui devrait avoir lieu est omise. Un utilisateur authentifié du serveur SQL peut créer de telle procédures temporaires. Ceci permet à un utilisateur authentifié mal intentionné d'exécuter n'importe quelle procédure appartenant au DBO

Si une base de donnée du serveur SQL appartient au compte « administrateur système », cela permet à un utilisateur mal intentionné d'utiliser les fonctions d'administration du serveur.

Il faut donc, pour cela, que les conditions suivantes soient réunies :

- Le propriétaire de la base de données doit être le compte administrateur système de la machine ;
- Le propriétaire de la procédure cataloguée doit être DBO ;
- L'utilisateur mal intentionné doit avoir un accès à la base de données, et doit pouvoir s'authentifier sur le serveur SQL.

5 Contournement provisoire

Vérifiez que le propriétaire de vos bases de données n'est jamais l'administrateur du système. Si l'une des bases de données appartient à l'administrateur système, changez le propriétaire immédiatement. Elle doit appartenir au compte d'un utilisateur sans privilège d'administration de Windows. On doit alors donner les droits du DBO à cet utilisateur.

6 Solution

Microsoft recommande d'appliquer le correctifs suivant dans tous les cas :

- Pour les système Intel :
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22470>
- Pour les systèmes alpha :
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22469>

Nota : Ces correctifs ne peuvent être installés que si vous avez appliqué le Service Pack 2 à votre serveur SQL.

7 Documentation

Bulletin de sécurité microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS00-048.asp>

La Faq à ce sujet :

<http://www.microsoft.com/technet/security/bulletin/fq00-048.asp>

Gestion détaillée du document

11 juillet 2000 version initiale.