Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2002
N° CERTA-2002-AVI-145

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft SQL Server

Gestion du document

Référence	CERTA-2002-AVI-145
Titre	Multiples vulnérabilités dans Microsoft SQL Server
Date de la première version	11 juillet 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-034 de Microsoft Bulletin de sécurité MS02-035 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.

2 Systèmes affectés

Microsoft SQL Server 7.0 et 2000.

3 Résumé

Plusieurs débordements de mémoire permettent à un utilisateur mal intentionné de prendre le contrôle de la base de données SQL ou du système.

Il est aussi possible d'obtenir des privilèges élevés au moyen d'une clé de la base de registre.

Enfin, il est possible de retrouver le mot de passe de l'administrateur du serveur (compte `sa`) pendant et après une installation ou une mise à jour de MSSQL. Dans certains cas le compte `sa` peut être le compte de l'administrateur du domaine.

4 Description

De nombreuses vulnérabilités de MSSQL Server permettent à un utilisateur mal intentionné de prendre le contrôle de la base de données, ou du système.

- Un débordement de mémoire dans la procédure de chiffrement des données d'authentification de MSSQL Server 2000 permet à un utilisateur mal intentionné d'obtenir le contrôle de la base de données, voire du serveur dans son ensemble selon la configuration du compte d'administration (`sa`).
- Un autre débordement de mémoire dans la procédure d'insertion de données dans les tables SQL sous MSSQL Server 2000 permet à un utilisateur mal intentionné de prendre le contrôle de la base de données voire du serveur dans son intégralité.
- Une mauvaise configuration des permissions sur les clés de la base de registre concernant le compte d'administration (`sa`) de MSQL Server 2000 permet à un utilisateur mal intentionné d'obtenir des privilèges plus élevés que ceux qui lui ont été attribués par l'administrateur. Il peut obtenir les privilèges du système d'exploitation lui-même.
- Lors de l'installation de MSSQL Server 7.0 ou MSDE 1.0 (*Microsoft Data Engine*) ou de MSSQL Server 2000 certaines informations concernant le compte de l'administrateur de serveur (`sa`), dont son mot de passe, sont stockées (parfois en clair) dans un fichier temporaire situé dans un répertoire accessible à n'importe quel utilisateur. Ce fichier n'est pas supprimé après l'installation.
- Toujours lors de l'installation de MSSQL Server 7.0 ou MSDE 1.0 (*Microsoft Data Engine*) ou de MSSQL Server 2000, un fichier journal est créé et contient lui aussi les mots de passe entrés dans le fichier de configuration.

`Nota` : Dans la plupart des cas, pour exploiter ces vulnérabilités, il faut pouvoir se connecter à la machine en local. Il n'est pas recommandé de laisser des utilisateurs, même sans privilège, se connecter localement sur un serveur.

5 Solution

Consulter les deux bulletins de sécurité Microsoft (voir paragraphe documentation) pour connaitre la disponibilité des différents correctifs selon les version et les vulnérabilités de MSSQL Server.

6 Documentation

- Bulletin de sécurité MS02-034 de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms02-034.asp
- Bulletin de sécurité MS02-035 de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms02-035.asp

Gestion détaillée du document

11 juillet 2002 version initiale.