Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 novembre 2001
N° CERTA-2001-INF-005

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Apparition de vers exploitant des vulnérabilités de MS-SQL Server

Gestion du document

Référence	CERTA-2001-INF-005
Titre	Apparition de vers exploitant des vulnérabilités de MS-SQL Server
Date de la première version	26 novembre 2001
Date de la dernière version	–
Source(s)	Microsoft TrendMicro
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

Propagation d'un ver de compromission :

- Exécution de code arbitraire ;
- Accès aux données ;
- Virus ;
- Déni de service ;
- Compromission ;
- Installation de portes dérobées.

2 Systèmes affectés

Serveur de base de données Microsoft SQL Server 6.5, 7.0 et 2000 avec le système d'authentification en Mode Mixte (*Mixed Mode*).

Attention : Le Mode Mixte est activé par défaut sur SQL Server 6.5, et le mot de passe du compte d'administration n'existe pas.

3 Résumé

Une faiblesse de la configuration de Microsoft SQL Server permet à des vers de se propager.
Un premier ver exploitant cette faille s'est répandu sur Internet.
Il est probable que des variantes apparaissent à l'avenir.

4 Description

Le ver utilise le fait que le Mode Mixte est activé et qu'il n'y a pas de mot de passe pour le Compte de Service (*Service Account* aussi appelé `sa`) de MS-SQL Server 6.5 par défaut.

Pour celà, il balaye des plages d'adresses IP à la recherche des serveurs dont le port 1433/TCP (SQL Server) est ouvert.

Si le mot de passe du compte `sa` est vide et si le Mode Mixte est activé (*Mixed-Mode*, voir l'avis CERTA-2000-AVI-063 à ce sujet), le ver peut exécuter la commande à distance SQL `XP_CMDSHELL` qui lui permet de se télécharger et s'installer sur le serveur victime.

Le ver actuellement connu télécharge deux exécutables : `DNSSERVICE.EXE` et `Win32Mon.exe`. Puis une clé de la base des registres est modifiée de façon à ce que le ver soit exécuté à chaque redémarrage du serveur.
(`\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TaskReg`)

Sous Windows 98 et Millenium Edition, le service est rendu « invisible » dans le gestionnaire des tâches.

Les exécutables téléchargés permettent aussi à un `bot` de se connecter à un réseau IRC et de rejoindre un canal pour attendre des commandes d'attaques en déni de service distribué ou autres malveillances.

5 Contournement provisoire

- Le mot de passe du compte `sa` doit être changé. Pour cela utiliser la procédure `sp_password Null,'nouveau-mot-de`
- L'authentification doit être faite par NTLM : désactiver le Mode Mixte du serveur SQL.
- Le port 1433/TCP doit être bloqué par le garde barrière pour éviter d'être attaqué depuis l'extérieur.
- Un serveur n'a aucune raison d'accepter d'exécuter des client (FTP, TFTP, etc.) et ne doit donc pas pouvoir télécharger les exécutables.
- Il vaut mieux installer le serveur sur un système acceptant le format de fichier NTFS, et restreindre les permissions à de certaines commandes, et fichiers.
- Sur le garde-barrière, bloquer la possibilité au serveur de se connecter en tant que client vers des ports IRC, FTP etc. (6669/TCP et supérieurs pour IRC, 21/TCP pour FTP, etc.).

6 Solution

Plusieurs vulnérabilités des serveurs MS-SQL très connues peuvent permettre à ce genre de ver de se propager, il faut donc appliquer les correctifs Microsoft comme indiqués dans les avis du CERTA :

- CERTA-2000-AVI-013 ;
- CERTA-2000-AVI-081 ;
- et CERTA-2001-AVI-063 ;

ou encore les bulletins de sécurité Microsoft

- MS00-035 ;
- MS00-041 ;
- MS00-048 ;
- MS00-092
- et MS01-032.

7 Documentation

- L'article de la base de connaissance de Microsoft concernant l'absence de mot de passe du compte `sa` sous MS-SQL Server :
  http://support.microsoft.com/support/kb/articles/Q274/7/73.ASP
- L'article de la base de connaissance de Microsoft concernant les permissions à appliquer sur certains fichiers de serveurs MS-SQL.
  http://support.microsoft.com/support/kb/articles/Q266/7/66.ASP
- Les Avis du CERTA cités ci-dessus :
  http://www.certa.ssi.gouv.fr
- Les bulletins de sécurité Microsoft cités ci-dessus :
  http://www.microsoft.com/technet/security/bulletin/

Gestion détaillée du document

26 novembre 2001 version initiale.