Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 juin 2002
N° CERTA-2002-ALE-006-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du ver Spida (Microsoft SQL Server)

Gestion du document

Référence	CERTA-2002-ALE-006-001
Titre	Propagation du ver Spida (Microsoft SQL Server)
Date de la première version	22 mai 2002
Date de la dernière version	04 juin 2002
Source(s)	Alerte "Microsoft SQL Spida Worm Propagation" d'ISS
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 du système ;
- déni de service.

2 Systèmes affectés

Serveur de base de données Microsoft SQL Server.

3 Résumé

Un ver exploitant une faiblesse dans la configuration de Microsoft SQL Server (compte `sa` sans mot de passe) se propage sur l'Internet. Ce type de ver n'est pas nouveau (se référer à la note d'information CERTA-2001-INF-005 "Apparition de vers exploitant des vulnérabilités de MS-SQL Server").

4 Description

Spida est un ver qui infecte les systèmes Microsoft SQL Server dont le Compte de Service (Service Account aussi appelé `sa`) ne possède pas de mot de passe, ce qui est la configuration par défaut.

La contamination des machines se fait en deux étapes :

- balayage d'une plage d'adresses IP tirée aléatoirement afin d'identifier des systèmes dont le port 1433/TCP (SQL Server) est ouvert ;
- infection d'un serveur vulnérable (compte `sa` sans mot de passe) : le ver utilise la procédure stockée étendue `xp_cmdshell` pour exécuter des commandes sur le système cible.

Le ver Spida collecte différentes informations relatives au système infecté (configuration réseau, mot de passe, etc) qui seront envoyé à une adresse mél avant de rechercher d'autres serveurs vulnérables à infecter.

La présence des fichiers dont les noms suivent est l'indication de la compromission du système par le ver Spida :

- `%Windir%\system32\drivers\services.exe`
- `%Windir%\system32\sqlprocess.js`
- `%Windir%\system32\sqlexec.js`
- `%Windir%\system32\sqldir.js`
- `%Windir%\system32\run.js`
- `%Windir%\system32\sqlinstall.bat`
- `%Windir%\system32\clemail.exe`
- `%Windir%\system32\pwdump2.exe`
- `%Windir%\system32\timer.dll`
- `%Windir%\system32\samdump.dll`

Trois clefs sont créées dans la base de registre :

- `HKLM\System\CurrentControlSet\Services\NetDDE\ImagePath`
- `HKLM\System\CurrentControlSet\Services\NetDDE\Start`
- `HKLM\software\microsoft\mssqlserver\client\connectto\dsquery`

5 Contournement provisoire

Bloquer le port 1433/TCP au niveau du garde-barrière afin d'empêcher l'exploitation de cette vulnérabilité depuis l'Internet.

6 Solution

Le compte `sa` doit posséder un mot de passe. Attention : utiliser un mot de passe résistant à l'attaque par force brute.

Ne pas oublier d'appliquer les différents correctifs relatifs à Microsoft SQL Server.

7 Documentation

- Alerte "Microsoft SQL Spida Worm Propagation" d'ISS :
  http://www.iss.net/security_center/alerts/advise118.php
- CERTA-2001-INF-005 "Apparition de vers exploitant des vulnérabilités de MS-SQL Server" :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-005/index.html
- Avis de McAfee "JS/SQL.Spida.b.worm" :
  http://vil.nai.com/vil/content/v_99499.htm

Gestion détaillée du document

22 mai 2002 version initiale.
04 juin 2002 correction du lien sur la note d'information dans la partie Documentation.