Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 janvier 2003
N° CERTA-2002-AVI-157-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft SQL Server 2000

Gestion du document

Référence	CERTA-2002-AVI-157-001
Titre	Multiples vulnérabilités dans Microsoft SQL Server 2000
Date de la première version	25 juillet 2002
Date de la dernière version	27 janvier 2003
Source(s)	Bulletin de securite de Microsoft #MS02-039
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 code arbitraire ;
- déni de service.

2 Systèmes affectés

Microsoft SQL Server 2000

3 Résumé

Trois vulnérabilités existent dans le service de résolution de Microsoft SQL Server 2000 permettant un déni de service ou l'exécution de code arbitraire sur le serveur.

4 Description

Microsoft SQL Server 2000 propose une fonction permettant de faire fonctionner plusieurs instances du service SQL sur le même serveur. Le port `1433/TCP` est alloué par défaut par le service SQL. Comme plusieurs instances

fonctionnent en même temps, elle ne peuvent pas toutes allouer le même port. Un service appellé SQL Server Resolution Service permet de diriger l'utilisateur vers le bon port, et donc la bonne instance. C'est ce service qui est vulnérable, il alloue le port `1434/UDP`.

Deux débordements de mémoire ainsi qu'une erreur de programmation permettent à un utilisateur mal intentionné de provoquer un déni de service, voire l'exécution de code arbitraire avec les droits de l'utilisateur ayant démarré le service SQL Server.

5 Contournement provisoire

Filtrer les ports `1433` et `1434 UDP` et `TCP` au niveau du garde-barrière afin d'empêcher l'exploitation de cette vulnérabilité depuis l'Internet.

6 Solution

Cette vulnérabilité est corrigée par le Service Pack 3 pour SQL Server.

Consulter le bulletin de sécurité #`MS02-039` de Microsoft pour connaitre la disponibilité des correctifs (voir la section Documentation).

7 Documentation

- Bulletin de sécurité de Microsoft #`MS02-039`
  http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
- Service Pack 3 pour SQL Server :
  http://www.microsoft.com/sql/downloads/2000/sp3.asp

Gestion détaillée du document

25 juillet 2002 version initiale.
27 janvier 2003 ajout du lien vers le service pack 3.