Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 décembre 2001
N° CERTA-2001-AVI-167

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le serveur SQL Microsoft

Gestion du document

Référence	CERTA-2001-AVI-167
Titre	Vulnérabilités dans le serveur SQL Microsoft
Date de la première version	24 décembre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-060
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

- Serveur Microsoft SQL 7.0 ;
- Serveur Microsoft SQL 2000.

3 Résumé

Deux vulnérabilités présentes dans le serveur Microsoft SQL permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou d'entraîner un deni de service sur la machine cible.

4 Description

- Première vulnérabilité :

Un utilisateur distant mal intentionné peut, par le biais d'un débordement de mémoire dans la gestion des requêtes, exécuter du code sur la machine cible avec les droits du serveur.

– Seconde vulnérabilité :
  L'environnement d'exécution des programmes C « runtime C » fonctionnant sous Windows 2000, XP et NT 4.0 contient une vulnérabilité de type « format string ».
  Un utilisateur distant mal intentionné peut, par le biais de cette vulnérabilité, créer un déni de service sur le serveur SQL.

5 Solution

Télécharger le correctif sur le site Microsoft :

– SQL Server 7.0 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=35066
– SQL Server 2000 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=35067
– Environnement d'exécution des programmes C « runtime C » :
  – Windows NT 4.0 et 2000 :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33500
  – Windows XP :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=35023

6 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-060.asp

Gestion détaillée du document

24 décembre 2001 version initiale.