



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 décembre 2000
N° CERTA-2000-AVI-081

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Microsoft SQL SERVER

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-AVI-081>

Gestion du document

Référence	CERTA-2000-AVI-081
Titre	Vulnérabilité sous Microsoft SQL SERVER
Date de la première version	05 décembre 2000
Date de la dernière version	–
Source(s)	Bulletin Microsoft (MS00-092)
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 7.0 et 2000 ;
- Microsoft SQL Server Desktop Engine 1.0 et 2000.

3 Résumé

Un utilisateur mal intentionné peut provoquer à distance un débordement de pile sur un serveur Microsoft SQL afin de créer un déni de service ou d'exécuter du code arbitraire.

4 Description

Des procédures Xps (Extended Stored Procedures) peuvent être installées sur un serveur Microsoft SQL afin d'apporter une amélioration des fonctionnalités.

Ces procédures ne vérifiant pas correctement certaines variables d'environnement un utilisateur distant peut provoquer un déni de service ou exécuter du code arbitraire.

L'exploitation de cette vulnérabilité n'est possible que si l'utilisateur mal intentionné possède une authentification sur le serveur ou, dans le cas d'un serveur SQL interfacé avec un site internet, s'il connaît exactement l'architecture du serveur.

5 Solution

Appliquer le correctif fourni par Microsoft (version US)
http://support.microsoft.com/support/sql/xp_security.asp

6 Documentation

Bulletin Microsoft :
<http://www.microsoft.com/technet/security/bulletin/ms00-092.asp>

La FAQ Microsoft :
<http://www.microsoft.com/technet/security/bulletin/fq00-092.asp>

Gestion détaillée du document

05 décembre 2000 version initiale.