Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juin 2002
N° CERTA-2002-AVI-123

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilités dans Microsoft SQLXML



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2002-AVI-123 |
| Titre | Vulnérabilités dans Microsoft SQLXML |
| Date de la première version | 13 juin 2002 |
| Date de la dernière version | – |
| Source(s) | Microsoft Security Bulletin #MS02-030 |
| 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 ;
- exécution de scripts sur un poste client ;
- élévation de privilèges.

## 2 Systèmes affectés

Différentes versions de Microsoft SQLXML, qui est un module de SQL Server 2000, sont vulnérables :
- Microsoft SQLXML contenu dans la suite SQL Server 2000 Gold ;
- Microsoft SQLXML version 1, 2 et 3.

## 3 Résumé

Deux vulnérabilités permettent d'exécuter du code arbitraire sur un serveur SQLXML ainsi que des scripts sur un client Internet Explorer.

# 4 Description

XML (eXtended Markup Language) permet d'échanger facilement des données structurées entre différentes architectures. SQLXML est un module de Microsoft SQL Server permettant de transmettre des données dans le format XML ainsi que d'accéder à la base SQL grâce à un navigateur HTTP.

Il existe deux vulnérabilités dans SQLXML :

- Un utilisateur mal intentionné peut exécuter du code arbitraire sur un serveur IIS au moyen d'un débordement de tampon ;
- Une vulnérabilité dans une fonction spécifiant une balise XML permet à un utilisateur mal intentionné d'exécuter des scripts sur un poste client.

# 5 Solution

Appliquer le correctif correspondant à votre version de SQLXML. Ces correctifs sont disponibles sur le site web de Microsoft.

# 6 Documentation

Consultez le site microsoft :
http://www.microsoft.com/technet/security/bulletin/MS02-030.asp

# Gestion détaillée du document

**13 juin 2002** version initiale.