Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 juillet 2008
N° CERTA-2008-AVI-356

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft SQL Server

Gestion du document

Référence	CERTA-2008-AVI-356
Titre	Multiples vulnérabilités dans Microsoft SQL Server
Date de la première version	09 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-040 du 08 juillet 2008
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 à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft SQL Server 7.0 ;
- Microsoft SQL Server 2000 ;
- Microsoft SQL Server 2005 ;
- Microsoft Data Engine (MSDE) 1.0 ;
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) ;
- Microsoft SQL Server 2005 Express Edition ;
- Microsoft SQL Server 2000 Desktop Engine (WMSDE) ;
- la base de données interne Windows (WYukon).

3 Résumé

Plusieurs vulnérabilités dans le serveur *Microsoft SQL Server* permettent à une personne malveillante d'effectuer une élévation de privilèges et d'exécuter du code arbitraire à distance.

4 Description

Des vulnérabilités affectent la réutilisation des pages, l'allocation de mémoire de la fonction *CONVERT*, la validation des fichiers sur disque avant leur chargement et la validation des instructions *INSERT*. Ces vulnérabilités permettent à une personne malveillante d'effectuer une élévation de privilèges et d'exécuter du code arbitraire.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-040 du 08 juillet 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-040.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-040.mspx
- Référence CVE CVE-2008-0085 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0085
- Référence CVE CVE-2008-0086 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0086
- Référence CVE CVE-2008-0106 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0106
- Référence CVE CVE-2008-0107 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0107

Gestion détaillée du document

09 juillet 2008 version initiale.