Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 février 2009
N° CERTA-2008-ALE-017-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft SQL Server

Gestion du document

Référence	CERTA-2008-ALE-017-001
Titre	Vulnérabilité dans Microsoft SQL Server
Date de la première version	12 décembre 2008
Date de la dernière version	11 février 2009
Source(s)	
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.

2 Systèmes affectés

- Microsoft SQL Server 2000 ;
- Microsoft SQL Server 2005 ;
- Microsoft SQL Server 2005 Express Edition ;
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000 et WMSDE) ;
- Windows Internal Database (WYukon).

Les systèmes Microsoft SQL Server 7.0 SP 4, Microsoft SQL Server 2005 SP3 et Microsoft SQL Server 2008 ne seraient pas affectés.

3 Résumé

Une vulnérabilité dans *Microsoft SQL Server* permet à une personne malintentionnée d'exécuter du code arbitraire.

4 Description

Une vulnérabilité de type débordement de mémoire dans la procédure stockée étendue *sp_replwritetovarbin()* de *Microsoft SQL Server* permet à une personne malintentionnée d'exécuter du code arbitraire.

Associée à une vulnérabilité de type injection de code SQL, cette vulnérabilité permet une exécution de code à distance.

5 Contournement provisoire

Il est recommandé de supprimer la procédure stockée étendue vulnérable ou d'en changer les droits d'exécution (cf. section Documentation).

Ceci peut entrainer des dysfonctionnements dans d'autres applications.

Les bonnes pratiques en matière de développement Web, notamment pour se protéger des injections SQL peuvent limiter les possibilités d'exploitation de cette vulnérabilité.

6 Solution

Se référer au bulletin de sécurité Microsoft MS09-004 pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Avis CERTA-2009-AVI-061 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-061/index.html
- Bulletin de sécurité Microsoft MS09-004 du 10 février 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-004.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-004.mspx
- Désactivation de procédures stockées étendues :
  http://msdn.microsoft.com/fr-fr/library/ms189506.aspx
- Avis de sécurité Microsoft 961040 du 22 décembre 2008 :
  http://www.microsoft.com/technet/security/advisory/961040.mspx
- Référence CVE CVE-5416:
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5416
- Bloc-notes MSRC, "Microsoft Security Advisory 961040" du 22 décembre 2008 :
  http://blogs.technet.com/msrc/archive/2008/12/22/microsoft-security-advisory-961040.aspx
- Bloc-notes SVRD, "More information about the SQL stored procedure vulnerability", 22 décembre 2008 :
  http://blogs.technet.com/swi/archive/2008/12/22/more-information-about-the-sql-stored-procedure-vulnerability.aspx

Gestion détaillée du document

12 décembre 2008 version initiale.

23 décembre 2008 ajout de la référence CVE, des liens Microsoft et mise à jour des versions vulnérables.

11 février 2009 ajout de la section solution et modification du CVE