



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 avril 2005
N° CERTA-2005-AVI-156-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans MySQL

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-2005-AVI-156>

Gestion du document

Référence	CERTA-2005-AVI-156-001
Titre	Multiples vulnérabilités dans MySQL
Date de la première version	26 avril 2005
Date de la dernière version	28 avril 2005
Source(s)	Bulletin de sécurité #234 du 25 avril 2005 Bulletin de sécurité #235 du 25 avril 2005 Bulletin de sécurité #236 du 26 avril 2005
Pièce(s) jointe(s)	

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

MySQL MaxDB versions antérieures à 7.5.00.26.

3 Résumé

Trois vulnérabilités découvertes dans MySQL MaxDB permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

MySQL MaxDB est un système de gestion de base de données.

- Une vulnérabilité de type débordement de mémoire présente dans la gestion des requêtes HTTP permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire, au moyen d'une requête GET HTTP malicieusement contruite ;
- deux vulnérabilités de type débordement de mémoire, présentes dans la fonctionnalité WebDAV permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

5 Solution

La version MySQL MaxDB 7.5.00.26 permet de corriger ces vulnérabilités (cf. section Documentation).

6 Documentation

- Site Internet de l'éditeur :
<http://dev.mysql.com>
- Mise à jour de sécurité MySQL MaxDB 7.5.00.26 :
<http://dev.mysql.com/downloads/maxdb/7.5.00.html>
- Bulletin de sécurité iDEFENSE #234 du 25 avril 2005 :
<http://www.odefense.com/application/poi/display?id=234&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #235 du 25 avril 2005 :
<http://www.odefense.com/application/poi/display?id=235&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #236 du 25 avril 2005 :
<http://www.odefense.com/application/poi/display?id=236&type=vulnerabilities>

Gestion détaillée du document

26 avril 2005 version initiale.

28 avril 2005 ajout d'une nouvelle vulnérabilité.