



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 20 juillet 2006  
N° CERTA-2006-AVI-305

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Cisco CS-MARS

---

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-2006-AVI-305>

---

### Gestion du document

Référence	CERTA-2006-AVI-305
Titre	Multiples vulnérabilités dans Cisco CS-MARS
Date de la première version	20 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #70728 du 19 juillet 2006
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 et en local ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

Toutes les versions de Cisco CS-MARS strictement antérieures à la version 4.2.1.

## 3 Résumé

Plusieurs vulnérabilités présentes dans Cisco CS-MARS permettent à un utilisateur mal intentionné d'exécuter du code arbitraire, de porter atteinte à la confidentialité des données ou d'élever ses privilèges.

## 4 Description

Cisco CS-MARS (Cisco Security Monitoring, Analysis and Response System) est un outil de supervision et de sécurisation de réseau.

Trois vulnérabilités sont présentes dans Cisco CS-MARS :

- CS-MARS comprend une base de données Oracle accessible via des comptes dont les mots de passe par défaut sont connus et triviaux. Un utilisateur mal intentionné peut donc utiliser ces comptes pour obtenir les informations contenues dans la base.
- CS-MARS comprend également l'application web JBoss. Une erreur dans cette application permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'une requête HTTP construite de façon particulière.
- Une erreur dans la ligne de commande CLI de CS-MARS permet à un utilisateur local authentifié d'élever ses privilèges et d'exécuter des commandes du super-utilisateur.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Cisco ID 70728 du 20 juillet 2006 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20060719-mars.shtml>

## **Gestion détaillée du document**

**20 juillet 2006** version initiale.