



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 31 décembre 2007  
N° CERTA-2007-AVI-571

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Mantis

---

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-2007-AVI-571>

---

### Gestion du document

Référence	CERTA-2007-AVI-571
Titre	Vulnérabilité de Mantis
Date de la première version	31 décembre 2007
Date de la dernière version	–
Source(s)	Note de la version 1.1 de Mantis
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

Injection de code indirecte (*cross-site scripting*).

## 2 Systèmes affectés

Mantis 1.0.x.

## 3 Résumé

Une vulnérabilité de Mantis permet à un utilisateur malveillant de réaliser de l'injection de code indirecte.

## 4 Description

Mantis est un logiciel de gestion d'anomalies des logiciels (*bug tracker*).

Lors du chargement d'un fichier sur le serveur, le programme *bug\_report.php* ne filtre pas le nom du fichier. Ce manque de vérification permet à un utilisateur malveillant de réaliser de l'injection de code indirecte.

## **5 Solution**

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

## **6 Documentation**

- Site de téléchargement du projet Mantis :  
<http://sourceforge.net/projects/mantisbt/>
- Note de version du projet Mantis :  
[http://www.mantisbt.org/bugs/changelog\\_page.php](http://www.mantisbt.org/bugs/changelog_page.php)

## **Gestion détaillée du document**

**31 décembre 2007** version initiale.