



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 septembre 2011  
N° CERTA-2011-AVI-506-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans MantisBT

---

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-2011-AVI-506>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2011-AVI-506-001                                      |
| Titre                       | Vulnérabilités dans MantisBT                                |
| Date de la première version | 13 septembre 2011   |
| Date de la dernière version | 23 septembre 2011   |
| Source                      | Annonce de la version 1.2.8 de MantisBT du 6 septembre 2011 |
| 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 ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

MantisBT 1.2.x.

## 3 Résumé

Plusieurs vulnérabilités affectent MantisBT et permettent en particulier de l'injection de code.

## 4 Description

Plusieurs vulnérabilités affectent le gestionnaire de bogues MantisBT :

- le défaut de validation des entrées dans plusieurs scripts PHP permet à un utilisateur malveillant de réaliser des injections de code indirectes à distance (XSS) ;

- le défaut de validation des entrées dans plusieurs scripts PHP permet à un utilisateur malveillant de parcourir l'arborescence du système de fichiers et d'inclure des fichiers (LFI ou *local file inclusion*).

## 5 Solution

La version 1.2.8 de MantisBT corrige ces vulnérabilités.

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

## 6 Documentation

- Annonce de la version 1.2.8 de MantisBT du 6 septembre 2011 :  
<http://www.mantisbt.org/>
- Bulletin de sécurité Debian DSA 2308 du 12 septembre 2011 :  
<http://www.debian.org/security/2011/dsa-2308>
- Référence CVE CVE-2011-3356 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3356>
- Référence CVE CVE-2011-3357 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3357>
- Référence CVE CVE-2011-3358 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3358>
- Référence CVE CVE-2011-3578 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3578>

## Gestion détaillée du document

**13 septembre 2011** version initiale.

**23 septembre 2011** ajout de références CVE.