

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-2010-AVI-473>

---

### Gestion du document

Référence	CERTA-2010-AVI-473
Titre	Vulnérabilités dans MantisBT
Date de la première version	06 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de version de MantisBT du 14 septembre 2010
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 à distance.

## 2 Systèmes affectés

MantisBT, versions antérieures à la version 1.2.3.

## 3 Résumé

MantisBT présente des vulnérabilités de type injection de code indirecte (XSS).

## 4 Description

MantisBT est un outil de gestion des erreurs de programme (*bug tracker*).

Des vulnérabilités de type XSS l'affectent :

- l'une d'elles réside dans la page de résumé d'un signalement (*summary*). Elle est exploitable par un utilisateur malveillant distant ;

- les autres, dans les composants *manage\_plugin\_uninstall.php*, *cfdef\_standard.php* et *print\_all\_bug\_page\_word.php*, sont exploitables par un administrateur authentifié.

## 5 Solution

La version MantisBT 1.2.3 remédie à ces vulnérabilités.

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

## 6 Documentation

- Bulletin de version de MantisBT du 14 septembre 2010 :  
[http://www.mantisbt.org/bugs/changelog\\_page.php?version\\_id=111](http://www.mantisbt.org/bugs/changelog_page.php?version_id=111)
- Site de téléchargement du projet MantisBT :  
<http://www.mantisbt.org/download.php>
- Référence CVE CVE-2010-3303 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3303>
- Référence CVE CVE-2010-3763 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3763>

## Gestion détaillée du document

**06 octobre 2010** version initiale.