



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 octobre 2010
N° CERTA-2010-AVI-418-001

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-2010-AVI-418>

Gestion du document

Référence	CERTA-2010-AVI-418-001
Titre	Vulnérabilités dans MantisBT
Date de la première version	06 septembre 2010
Date de la dernière version	06 octobre 2010
Source(s)	Bulletin de version de MantisBT du 29 juillet 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 1.2.2.

3 Résumé

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

4 Description

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

Deux vulnérabilités de type XSS l'affectent :

- le rendu des pièces jointes intégrées permet l'injection de code HTML ou de scripts ;
- la fonction `project_id_filter_target` permet de réaliser de l'injection de code indirecte quand le filtrage avancé des vues est utilisé.

5 Solution

La version MantisBT 1.2.2 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 29 juillet 2010 :
http://www.mantisbt.org/bugs/changelog_page.php?version_id=110
- Site de téléchargement du projet MantisBT :
<http://www.mantisbt.org/download.php>
- Référence CVE CVE-2010-2802 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2802>
- Référence CVE CVE-2010-2574 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2574>

Gestion détaillée du document

06 septembre 2010 version initiale.

06 octobre 2010 ajout des références CVE.