

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-612>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2010-AVI-612-001 |
| Titre | Vulnérabilités dans MantisBT |
| Date de la première version | 06 janvier 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletin de la version 1.2.4 de MantisBT du 15 décembre 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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

MantisBT, version 1.2.3 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans MantisBT permettent à un utilisateur malveillant de contourner la politique de sécurité ou de faire de l'injection de code indirecte.

4 Description

Plusieurs vulnérabilités affectent MantisBT :

- des erreurs dans le programme *upgrade_unattended.php* permettent de réaliser de l'injection de code indirecte (XSS), de l'inclusion locale de code et d'atteindre sans droit des fichiers ;

- quand le paramètre *report_stay* est à 1 (un), une injection de code indirecte est possible ;
- le codage imparfait des adresses IRC permet de réaliser de l'injection de code indirecte.

5 Solution

La version 1.2.4 de MantisBT corrige ces problèmes.

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

6 Documentation

- Bulletin de la version 1.2.4 de MantisBT du 15 décembre 2010 :
http://www.mantisbt.org/bugs/changelog_page.php?project=mantisbt&version=1.2.4
- Bulletins de sécurité Fedora FEDORA-2010-19070 et FEDORA-2010-19078 du 19 décembre 2010 :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052721.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052730.html>
- Référence CVE CVE-2010-4348 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4348>
- Référence CVE CVE-2010-4349 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4349>
- Référence CVE CVE-2010-4350 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4350>

Gestion détaillée du document

16 décembre 2010 version initiale.

06 janvier 2011 ajout des références aux bulletins Fedora et aux CVE.