



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 avril 2011
N° CERTA-2011-AVI-258

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans BestPractical RT

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-258>

Gestion du document

Référence	CERTA-2011-AVI-258
Titre	Vulnérabilités dans BestPractical RT
Date de la première version	27 avril 2011
Date de la dernière version	–
Sources	Bulletins de sécurité BestPractical du 14 avril 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

BestPractical RT (Request Tracker) 2.0.x, 3.6.x, 3.8.x, 4.0.0rcx.

3 Résumé

Plusieurs vulnérabilités affectent BestPractical RT permettant des injections de code et la lecture sans droit de données sensibles.

4 Description

Plusieurs vulnérabilités affectent BestPractical RT :

- quand l'option *CustomFieldValuesSources* est activée, un utilisateur malveillant peut réaliser des injections de requêtes illégitime par rebond ;
- des injections de requêtes SQL sont possibles ;
- l'interface de recherche permet d'obtenir des informations sensibles, comme des mots de passe ;
- un utilisateur malveillant peut lire n'importe quel fichier du serveur par le biais d'une requête HTTP spécialement formée ;
- plusieurs vulnérabilités (XSS) permettent à un utilisateur malveillant de réaliser de l'injection de code indirecte ;
- il est possible de transmettre les informations de connexion des utilisateurs sur un serveur externe, de manière illégitime.

5 Solution

Les versions 3.6.11, 3.8.10 et 4.0.0rc8 de BestPractical RT corrigent ces problèmes.

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

6 Documentation

- Bulletins de sécurité BestPractical du 14 avril 2011 :
<http://lists.bestpractical.com/pipermail/rt-announce/2011-April/000187.html>
<http://lists.bestpractical.com/pipermail/rt-announce/2011-April/000188.html>
<http://lists.bestpractical.com/pipermail/rt-announce/2011-April/000189.html>
- Référence CVE CVE-2011-1685 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1685>
- Référence CVE CVE-2011-1686 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1686>
- Référence CVE CVE-2011-1687 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1687>
- Référence CVE CVE-2011-1688 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1688>
- Référence CVE CVE-2011-1689 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1689>
- Référence CVE CVE-2011-1690 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1690>

Gestion détaillée du document

27 avril 2011 version initiale.