Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juin 2010
N° CERTA-2010-AVI-290-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabiltés dans Bugzilla

Gestion du document

Référence	CERTA-2010-AVI-290-001
Titre	Vulnérabiltés dans Bugzilla
Date de la première version	28 juin 2010
Date de la dernière version	08 juillet 2010
Source	Bulletin de sécurité Bugzilla du 24 juin 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

Atteinte à la confidentialité des données.

2 Systèmes affectés

Bugzilla 3.2.x, 3.4.x, 3.6.x, 3.7.x.

3 Résumé

Deux vulnérabilités dans Bugzilla permettent à un utilisateur malveillant de porter atteinte à la confidentialité de données.

4 Description

Quand le paramètre de configuration `$use_suexec` est positionné à 1 (un), le fichier de configuration devient lisible par tous. Les mots de passe et les informations de protection contre les requêtes illégitimes par rebond (CSRF) deviennent visibles (CVE-2010-0180).

Un problème dans la gestion des URL de recherche permet à un utilisateur n'appartenant pas au groupe `time tracking group` d'obtenir des informations réservées à ce dernier (CVE-2010-1204).

5 Solution

Les versions 3.2.7, 3.4.7, 3.6.1 et 3.7.1 corrigent ces problèmes.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Bugzilla du 24 juin 2010 :
  http://www.bugzilla.org/security/3.2.6/
- Référence CVE CVE-2010-0180 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0180
- Référence CVE CVE-2010-1204 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1204
- Bulletin de sécurité Fedora FEDORA-2010-10398 du 25 juin 2010 :
  https://admin.fedoraproject.org/updates/bugzilla-3.4.7-1.fc12

Gestion détaillée du document

28 juin 2010 version initiale.
08 juillet 2010 ajout de la référence pour la mise à jour Fedora.