Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 février 2012
N° CERTA-2012-AVI-053

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Bugzilla

Gestion du document

Référence	CERTA-2012-AVI-053
Titre	Vulnérabilités dans Bugzilla
Date de la première version	03 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bugzilla du 31 janvier 2012
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 requêtes illégitime par rebond.

2 Systèmes affectés

- Bugzilla 2.x ;
- Bugzilla 3.x ;
- Bugzilla 4.x.

3 Résumé

Deux vulnérabilités ont été corrigées dans Bugzilla. Elles peuvent être utilisées par une personne distante malintentionnée pour réaliser de l'injection de requêtes illégitime par rebond (CSRF) et pour contourner la politique de sécurité.

4 Description

Deux vulnérabilités ont été corrigées dans Bugzilla. La première est due à un mauvais contrôle des caractères contenus dans une adresse de messagerie lors de la création d'un compte. Un attaquant peut ainsi utiliser des caractères utf8 semblables à des caractéres ASCII pour usurper l'adresse d'un autre compte. La seconde vulnérabilité est due à un mauvais contrôle de certaines entrées et peut être utilisée pour faire de l'injection de requêtes illégitime par rebond.

5 Solution

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

6 Documentation

- Bulletin de sécurité Bugzilla du 31 janvier 2012 :
  http://bugzilla.org/security/3.4.13
- Référence CVE CVE-2012-0440 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0440
- Référence CVE CVE-2012-0448 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0448

Gestion détaillée du document

03 février 2012 version initiale.