Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2009
N° CERTA-2009-AVI-391-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Bugzilla

Gestion du document

Référence	CERTA-2009-AVI-391-001
Titre	Multiples vulnérabilités dans Bugzilla
Date de la première version	18 septembre 2009
Date de la dernière version	19 octobre 2009
Source(s)	Bulletin de sécurité Bugzilla du 11 septembre 2009
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 l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- *Bugzilla* 3.0.8 ;
- *Bugzilla* 3.2.4 ;
- *Bugzilla* 3.4.1.

3 Résumé

Plusieurs vulnérabilités présentes dans *Bugzilla* permettent à un utilisateur distant malintentionné de porter atteinte à la confidentialité ou à l'intégrité des données.

4 Description

Trois vulnérabilités sont présentes dans *Bugzilla* :

- la première concerne un manque de contrôle dans certaines entrées passées au service *Bug.search* et permet d'injecter des commandes SQL ;
- la seconde est relative à un manque de contrôle dans certaines entrées passées au service *Bug.create* et permet d'injecter des commandes SQL ;
- la dernière est relative au mécanisme de gestion des mots de passe des utilisateurs qui, sous certaines conditions, affiche des mots de passe en clair.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
Les versions 3.0.9, 3.2.5 et 3.4.2 corrigent le problème :
http://www.bugzilla.com/download/

6 Documentation

- Bulletin de sécurité Bugzilla du 11 septembre 2009 :
  http://www.bugzilla.com/security/3.0.8
- Bulletin de sécurité Debian DSA-1913-1 du 17 octobre 2009 :
  http://www.debian.org/security/2009/dsa-1913
- Référence CVE CVE-2009-3125 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3125
- Référence CVE CVE-2009-3165 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3165
- Référence CVE CVE-2009-3166 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3166

Gestion détaillée du document

18 septembre 2009 version initiale.
19 octobre 2009 ajout de la référence au bulletin de sécurité Debian.