



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 août 2010
N° CERTA-2010-AVI-362

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Bugzilla

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-362>

Gestion du document

Référence	CERTA-2010-AVI-362
Titre	Vulnérabilités dans Bugzilla
Date de la première version	09 août 2010
Date de la dernière version	–
Source(s)	Avis de sécurité Bugzilla du 05 août 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 ;
- atteinte à la confidentialité des données ;
- deni de service.

2 Systèmes affectés

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

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans *Bugzilla*.

4 Description

Plusieurs failles dans *Bugzilla* permettent à une personne malintentionnée de contourner la politique de sécurité et de porter atteinte à la confidentialité des données. Une vulnérabilité concernant les configurations utilisant

PostgreSQL permet également à des personnes d'empêcher le visionnage de bugs en y insérant des commentaires spécialement conçus.

5 Solution

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

6 Documentation

- Avis de sécurité Bugzilla du 05 août 2010 :
<http://www.bugzilla.org/security/3.2.7/>
- Référence CVE CVE-2010-2756 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2756>
- Référence CVE CVE-2010-2757 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2757>
- Référence CVE CVE-2010-2758 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2758>
- Référence CVE CVE-2010-2759 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2759>

Gestion détaillée du document

09 août 2010 version initiale.