



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 2009  
N° CERTA-2009-AVI-046

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de 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-2009-AVI-046>

---

### Gestion du document

Référence	CERTA-2009-AVI-046
Titre	Vulnérabilités de Bugzilla
Date de la première version	03 février 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité du projet Bugzilla des 02 et 03 février 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

Bugzilla 3.x et 2.x.

## 3 Résumé

Plusieurs vulnérabilités affectent Bugzilla. Elles permettent des injections de code indirectes et des requêtes illégitimes par rebond.

## 4 Description

Plusieurs vulnérabilités sont présentes dans l'outil de gestion des bogues Bugzilla :

- un manque de validation dans la gestion des pièces jointes permet à un utilisateur malveillant de fabriquer des requêtes illégitimes par rebond (CRSF ou *cross-site request forgery*) ;

- un manque de validation dans la gestion des pièces jointes permet également à un utilisateur malveillant de réaliser de l'injection de code indirecte (XSS ou *cross-site scripting*);
- quand le module *mod\_perl* est utilisé, les chaînes de caractères ne sont pas suffisamment aléatoires, ce qui permet de fabriquer des requêtes illégitimes par rebond et la visualisation de pièces jointes non publiques.

## 5 Solution

Les versions 2.22.7, 3.0.8, 3.2.2 et 3.3.3 corrigent ces vulnérabilités. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité du projet Bugzilla du 02 février 2009 :  
<http://www.bugzilla.org/security/2.22.6/>
- Bulletin de sécurité du projet Bugzilla du 03 février 2009 :  
<http://www.bugzilla.org/security/3.0.7/>

## Gestion détaillée du document

**03 février 2009** version initiale.