



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 04 novembre 2010  
N° CERTA-2010-AVI-533

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-533>

---

### Gestion du document

Référence	CERTA-2010-AVI-533
Titre	Multiples vulnérabilités dans Bugzilla
Date de la première version	04 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bugzilla du 2 novembre 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 ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

Bugzilla versions :

- 3.2.x antérieures à 3.2.9 ;
- 3.4.x antérieures à 3.4.9 ;
- 3.6.x antérieures à 3.6.3.

## 3 Résumé

Trois failles ont été corrigées dans *Bugzilla* dont l'exploitation permet, entre autres, l'injection de code indirecte à distance.

## 4 Description

Une erreur dans la validation d'une entrée non spécifiée par l'éditeur permet d'insérer des en-têtes arbitraires dans la réponse retournée par le serveur à l'utilisateur. Une personne malintentionnée peut réaliser par ce biais une injection de code indirecte à distance (CVE-2010-3172).

Les noms des graphes créés dans le répertoire `graphs/` sont prédictibles. Il est alors possible à un utilisateur non autorisé d'accéder à ces graphes (CVE-2010-3764).

Enfin, une vulnérabilité permettant l'injection de code indirecte à distance affecte la version 2.8.1 de la *Yahoo! UI Library* qui est incluse dans Bugzilla.

## 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 2 novembre 2010  
<http://www.bugzilla.org/security/3.2.8/>
- Référence CVE CVE-2010-3172 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3172>
- Référence CVE CVE-2010-3764 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3764>

## Gestion détaillée du document

**04 novembre 2010** version initiale.