

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-2005-AVI-261>

---

### Gestion du document

Référence	CERTA-2005-AVI-261
Titre	Multiples vulnérabilités dans Bugzilla
Date de la première version	15 juillet 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA 200507-12 du 13 juillet 2005
Pièce(s) jointe(s)	

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.

## 2 Systèmes affectés

- Pour la branche stable Bugzilla version 2.18.1 et versions antérieures sont vulnérables ;
- pour la branche instable; Bugzilla version 2.19.3 et versions antérieures sont vulnérables ;
- une récente vulnérabilité décrite dans cet avis affecte la branche stable Bugzilla 2.18.2 et versions antérieures.

## 3 Résumé

Deux vulnérabilités découvertes dans Bugzilla permet à un utilisateur distant mal intentionné de contourner la politique de sécurité et/ou de porter atteinte à la confidentialité des données.

## 4 Description

Bugzilla est un programme qui permet le suivi des erreurs de programmation et des vulnérabilités.

- Une vulnérabilité dans Bugzilla permet à un individu malintentionné de contourner la politique de sécurité afin de modifier les valeurs affectés à un rapport de vulnérabilité ou d'erreur de programmation (CAN-2005-2173);
- une seconde vulnérabilité permet à un utilisateur distant mal intentionné de porter atteinte à la confidentialité des données en manipulant malicieusement l'adresse réticulaire (URL) (CAN-2005-2174).

## 5 Solution

Mettre à jour Bugzilla en version 2.18.3 (pour la branche stable) et en version 2.20.rc1 (pour la branche instable).

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

## 6 Documentation

- Bulletin de sécurité Gentoo GLSA 200507-12 du 13 juillet 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200507-12.xml>
- Bulletin de sécurité Bugzilla du 07 juillet 2005 :  
<http://www.bugzilla.org/security/2.18.1/>
- Référence CVE CAN-2005-2173 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2173>
- Référence CVE CAN-2005-2174 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2174>

## Gestion détaillée du document

**15 juillet 2005** version initiale.