Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 août 2007
N° CERTA-2007-AVI-379

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Bugzilla

Gestion du document

Référence	CERTA-2007-AVI-379
Titre	Multiples vulnérabilités de Bugzilla
Date de la première version	27 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Bugzilla du 23 août 2007
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

- Injection de code indirecte (*cross site scripting*) ;
- exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Bugzilla, versions 2.x et 3.x.

3 Résumé

Plusieurs vulnérabilités de *Bugzilla* permettent à un utilisateur malveillant de réaliser des injections de code indirectes, de divulguer de données ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent *Bugzilla* :

- une gestion incorrecte des entrées dans le formulaire de signalement de bogue permet à un utilisateur malveillant de réaliser une injection de code indirecte ;

– un filtrage insuffusant des entrées dans une fonctionnalité de courrier électronique permet l'exécution de code arbitraire à distance ;
– l'interface XML-RPC permet à des utilisateurs non autorisés des données confidentielles.

5 Solution

Les versions 2.20.5, 2.22.3, 3.0.1 et 3.1.1 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 23 août 2007 :
http://www.bugzilla.org/security/2.20.4/

Gestion détaillée du document

27 août 2007 version initiale.