Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2011
N° CERTA-2011-AVI-031

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Bugzilla

Gestion du document

Référence	CERTA-2011-AVI-031
Titre	Multiples vulnérabilités dans Bugzilla
Date de la première version	25 janvier 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bugzilla du 24 janvier 2011
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 ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

- Bugzilla versions 4.x antérieures à la version 4.0rc2 ;
- Bugzilla versions 3.6.x antérieures à la version 3.6.4 ;
- Bugzilla versions 3.4.x antérieures à la version 3.4.10 ;
- Bugzilla versions 3.2.x antérieures à la version 3.2.10.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Bugzilla. L'une d'entre elles permet à un utilisateur de récupérer les privilèges d'un autre compte.

4 Description

Plusieurs vulnérabilités ont été corrigées dans Bugzilla.

Une vulnérabilité non spécifiée permet à un utilisateur de récupérer les privilèges d'un autre compte.

Une erreur dans la validation de certaines entrées non spécifiées par l'éditeur permet d'insérer du contenu et des en-têtes arbitraires dans la réponse retournée par le serveur à l'utilisateur.

D'autres vulnérabilités permettant l'injection de code indirecte à distance et l'injection de requêtes illégitime par rebond ont également été corrigées.

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 24 janvier 2011 :
  http://www.bugzilla.org/security/3.2.9/
- Référence CVE CVE-2010-4568 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4568
- Référence CVE CVE-2010-2761 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2761
- Référence CVE CVE-2010-4411 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4411
- Référence CVE CVE-2010-4572 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4572
- Référence CVE CVE-2010-4569 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4569
- Référence CVE CVE-2010-4570 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4570
- Référence CVE CVE-2010-4567 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4567
- Référence CVE CVE-2011-0048 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0048
- Référence CVE CVE-2011-0046 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0046

Gestion détaillée du document

25 janvier 2011 version initiale.