Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 août 2011
N° CERTA-2011-AVI-430

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Multiples vulnérabilités dans Bugzilla



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2011-AVI-430 |
| Titre | Multiples vulnérabilités dans Bugzilla |
| Date de la première version | 05 août 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Bugzilla du 4 aout 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 ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- Bugzilla version 3.4.x antérieures à la version 3.4.12 ;
- Bugzilla version 3.6.x antérieures à la version 3.6.6 ;
- Bugzilla version 4.0.x antérieures à la version 4.0.2 ;
- Bugzilla version 4.1.x antérieures à la version 4.1.3.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Bugzilla.

# 4 Description

Plusieurs vulnérabilités ont été corrigées dans Bugzilla dont :

- une mauvaise validation de certains éléments permet de mener des attaques par injection de code indirecte ;
- Il est possible de déterminer l'existence d'éléments confidentiels lors de la création ou de la mise à jour de bugs ;
- Une mauvaise gestion de fichiers temporaires peut être exploitées par des utilisateurs locaux pour porter atteinte à la confidentialité des données.

Se référer au bulletin de l'éditeur pour plus de détails sur les vulnérabilités corrigées et les versions affectées par ces vulnérabilités.

# 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
Les versions 3.4.12, 3.6.6, 4.0.2 et 4.1.3 corrigent ces vulnérabilités.

# 6 Documentation

- Bulletin de sécurité Bugzilla du 04 août 2011 :
  http://www.bugzilla.org/security/3.4.11/
- Référence CVE CVE-2011-2379 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2379
- Référence CVE CVE-2011-2380 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2380
- Référence CVE CVE-2011-2381 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2381
- Référence CVE CVE-2011-2976 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2976
- Référence CVE CVE-2011-2977 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2977
- Référence CVE CVE-2011-2978 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2978
- Référence CVE CVE-2011-2979 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2979

# Gestion détaillée du document

**05 août 2011** version initiale.