



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 août 2010  
N° CERTA-2010-AVI-354

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans JBoss Enterprise SOA

---

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-354>

---

### Gestion du document

Référence	CERTA-2010-AVI-354
Titre	Vulnérabilités dans JBoss Enterprise SOA
Date de la première version	04 août 2010
Date de la dernière version	–
Source(s)	Note de changements de la version 5.0.2 de JBoss Enterprise SOA
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

Les versions antérieures des produits suivants :

- JBoss EAP 5.0.1 ;
- JBoss ESB 4.7 CPO02 ;
- JBoss Rules 5.0.1 ;
- JBoss jBPM 3.2.9 ;
- Apache jUDDI 3.0.1 ;
- PicketLink 1.0.

## 3 Résumé

De nombreuses corrections ont été apportées à JBoss Enterprise SOA, dont deux concernant des vulnérabilités permettant le contournement de la politique de sécurité et l'élévation de privilèges.

## 4 Description

De nombreuses corrections ont été apportées à JBoss Enterprise SOA, dont deux concernant des vulnérabilités associées aux CVE CVE-2010-2474 et CVE-2010-2493. Ces vulnérabilités permettent à une personne malintentionnée de contourner la politique de sécurité ou d'élever ses privilèges. Les correctifs portent sur les bogues suivants : JBESB-3280, JBESB-3290, JBESB-3296, JBESB-3301, JBESB-3337, JBESB-3345, JBESB-3347, JBPM-2828, JBESB-2442, JBESB-2911, JBESB-3028, JBESB-3035, JBESB-3038, JBESB-3257, JBESB-3263, JBESB-3282, JBESB-3288, JBESB-3300, JBESB-3317, JBESB-3326, JBESB-3346, JBESB-3349, JBIDE-5596, JBIDE-5597, JBPAPP-3002, JOPR-419, SOA-952, SOA-1077, SOA-1168, SOA-1445, SOA-1446, SOA-1549, SOA-1564, SOA-1600, SOA-1623, SOA-1673, SOA-1711, SOA-1867, SOA-1916, SOA-1970, SOA-1981, SOA-2007, SOA-2029, SOA-2034, SOA-2083, SOA-2084, SOA-2086, SOA-2099, SOA-2105, SOA-2114, SOA-2120.

## 5 Solution

Se référer à la note de changements de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Note de changements de JBoss Enterprise SOA 5.0.2 :  
[http://www.redhat.com/docs/en\\_US/JBoss\\_SOA\\_Platform/5.0.2/html/5.0.2\\_Release\\_Notes/index.html](http://www.redhat.com/docs/en_US/JBoss_SOA_Platform/5.0.2/html/5.0.2_Release_Notes/index.html)
- Référence CVE CVE-2010-2474 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2474>
- Référence CVE CVE-2010-2493 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2493>

## Gestion détaillée du document

04 août 2010 version initiale.