



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 août 2011
N° CERTA-2011-AVI-454

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Apache Tomcat

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-2011-AVI-454>

Gestion du document

Référence	CERTA-2011-AVI-454
Titre	Vulnérabilités dans Apache Tomcat
Date de la première version	16 août 2011
Date de la dernière version	–
Source(s)	http://tomcat.apache.org/security-7.html
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 l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Apache Tomcat 7.0.0-7.0.19 ;
- Apache Tomcat 6.0.0-6.0.32 ;
- Apache Tomcat 5.5.0-5.5.33.

3 Résumé

De multiples vulnérabilités présentes dans le produit *Apache Tomcat* ont été corrigées. Elles permettent la divulgation de mots de passe utilisateur, l'altération de fichiers de configuration et le contournement de la politique de sécurité.

4 Description

De multiples vulnérabilités présentes dans le produit *Apache Tomcat* ont été corrigées. Ces vulnérabilités permettent la divulgation et/ou l'altération d'information. Il convient néanmoins de détailler les informations à risque :

- contournement de la politique de sécurité permettant l'accès à des fichiers protégés du super-utilisateur (root) (CVE-2011-2729, CVE-2011-2526) ;
- divulgation du mot de passe de l'utilisateur (CVE-2011-2204) ;
- divulgation (et/ou modification) des fichiers `web.xml`, `context.xml` et fichiers `tld` d'autres applications web de l'instance *Apache Tomcat* (CVE-2011-2481).

5 Solution

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

Il est important de noter, que suivant la documentation de l'éditeur (<http://tomcat.apache.org/security-5.html>), les mises à jour ne sont pas encore disponibles pour les versions 5.X de *Apache Tomcat*. Celles-ci seront disponibles lors de la publication de la version 5.5.34 de *Apache Tomcat* (à paraître).

6 Documentation

- Référence CVE CVE-2011-2481 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2481>
- Référence CVE CVE-2011-2204 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2204>
- Référence CVE CVE-2011-2526 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2526>
- Référence CVE CVE-2011-2729 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2729>

Gestion détaillée du document

16 août 2011 version initiale.