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 octobre 2009
N° CERTA-2009-AVI-211-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Apache Tomcat

Gestion du document

Référence	CERTA-2009-AVI-211-001
Titre	Multiples vulnérabilités de Apache Tomcat
Date de la première version	08 juin 2009
Date de la dernière version	27 octobre 2009
Source(s)	Bulletins de sécurité Apache Tomcat du 03 juin 2009
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

- Déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- injection de code indirecte.

2 Systèmes affectés

- Apache Tomcat versions 4.1.39 et antérieures ;
- Apache Tomcat versions 5.5.27 et antérieures ;
- Apache Tomcat versions 6.0.18 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans `Apache Tomcat` permettent à un utilisateur distant de provoquer un déni de service et de porter atteinte à la confidentialité et à l'intégrité des données.

4 Description

Plusieurs vulnérabilités sont présentes dans `Apache Tomcat` :

- la première est relative à une erreur dans le traitement de certains en-têtes `HTTP` par le composant `AJP Connector`. Elle permet à un utilisateur distant de provoquer un déni de service ;
- la deuxième concerne certaines fonctionnalités d'authentification et permet à un personne distante d'obtenir des identifiants valides d'utilisateur via des requêtes particulières ;
- la troisième est relative à la gestion des fichiers *web.xml* et *tld* qui peuvent être modifiés par une application particulière dans une autre application si celles-ci sont dans la même instance de `Tomcat` ;
- la quatrième est due à une vulnérabilité dans le *RequestDispatcher* et permet à un utilisateur malintentionné d'accéder à des données sensibles ;
- la dernière est due à une erreur dans le calendrier permettant de réaliser une attaque par injection de code indirecte.

5 Solution

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

6 Documentation

- Bulletins de sécurité Tomcat :
  http://tomcat.apache.org/security-4.html
  http://tomcat.apache.org/security-5.html
  http://tomcat.apache.org/security-6.html
- Bulletins de sécurité Tomcat du 03 juin 2009 :
  http://marc.info/?l=tomcat-user&m=124404378413736&w=2
  http://marc.info/?l=tomcat-user&m=124404378913734&w=2
  http://marc.info/?l=tomcat-user&m=124412001618125&w=2
- Bulletin de sécurité HP-UX du 21 octobre 2009 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01908935
- Référence CVE CVE-2008-5515 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5515
- Référence CVE CVE-2009-0033 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0033
- Référence CVE CVE-2009-0580 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0580
- Référence CVE CVE-2009-0781 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0781
- Référence CVE CVE-2009-0783 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0783

Gestion détaillée du document

08 juin 2009 version initiale ;
27 ocotbre 2009 ajout de référence CVE et du bulletin HP-UX.