



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 octobre 2008
N° CERTA-2008-AVI-392-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2008-AVI-392>

Gestion du document

Référence	CERTA-2008-AVI-392-001
Titre	Multiples vulnérabilités dans Apache Tomcat
Date de la première version	07 août 2008
Date de la dernière version	06 octobre 2008
Source(s)	Bulletins de mise à jour Apache Tomcat
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.

2 Systèmes affectés

- Apache Tomcat version 4.1.37 et versions antérieures ;
- Apache Tomcat version 5.5.26 et versions antérieures ;
- Apache Tomcat version 6.0.16 et versions antérieures.

3 Résumé

Deux vulnérabilités ont été découvertes dans le serveur web *Apache Tomcat*. Ces vulnérabilités peuvent être exploitées afin de contourner la politique de sécurité.

4 Description

Deux vulnérabilités ont été découvertes dans les versions 4, 5 et 6 d'*Apache Tomcat* :

- la première vulnérabilité est due à une mauvaise gestion des arguments passés à la fonction

`HttpServletResponse.sendError()`. Cette vulnérabilité peut être exploitée afin de réaliser une attaque par injection de code indirecte (*Cross Site Scripting*);

- la seconde vulnérabilité permet d'atteindre des ressources en accès restreint.

5 Solution

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

6 Documentation

- Bulletins de mise à jour Apache Tomcat :
 - <http://tomcat.apache.org/security-4.html>
 - <http://tomcat.apache.org/security-5.html>
 - <http://tomcat.apache.org/security-6.html>
- Bulletin de sécurité Debian DSA-1593 du 09 juin 2008 :
<http://www.debian.org/security/2008/dsa-1593>
- Bulletins de sécurité Fedora FEDORA-2008-7977 du 11 septembre 2008 :
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00712.html>
- Bulletins de sécurité Fedora FEDORA-2008-8113 du 16 septembre 2008 :
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00859.html>
- Bulletins de sécurité Fedora FEDORA-2008-8130 du 16 septembre 2008 :
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00889.html>
- Bulletin de sécurité Mandriva MDVSA-2008:188 du 05 septembre 2008 :
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité RedHat RHSA-2008:0648 du 27 août 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0648.html>
- Bulletin de sécurité Suse SUSE-SR:2008:014 du 04 juillet 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-07/msg00001.html>
- Bulletin de sécurité Suse SUSE-SR:2008:018 du 19 septembre 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html>
- Référence CVE CVE-2008-1232 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1232>
- Référence CVE CVE-2008-1947 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1947>
- Référence CVE CVE-2008-2370 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2370>

Gestion détaillée du document

07 août 2008 version initiale.

06 octobre 2008 ajout des références aux distributions Linux.