

[NEWS] Tomcat Documentation XSS Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00032.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 21 May 2007 10:17:24 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Tomcat Documentation XSS Vulnerabilities

SUMMARY

The Tomcat documentation web application includes a sample application that contains multiple XSS vulnerabilities.

DETAILS

Vulnerable Systems:

- * Tomcat versions from 4.0.0 to 4.0.6
- * Tomcat versions from 4.1.0 to 4.1.36
- * Tomcat versions from 5.0.0 to 5.0.30
- * Tomcat versions from 5.5.0 to 5.5.23
- * Tomcat versions from 6.0.0 to 6.0.10

Immune Systems:

- * Tomcat version 4.0.7
- * Tomcat version 4.1.37
- * Tomcat version 5.0.31
- * Tomcat version 5.5.24
- * Tomcat version 6.0.11

[NEWS] Tomcat Documentation XSS Vulnerabilities

The JSP and Servlet included in the sample application within the Tomcat documentation webapp did not escape user provided data before including it in the output. This enabled a XSS attack. These pages have been simplified not to use any user provided data in the output.

Example:

[http://server/tomcat-docs/appdev/sample/web/hello.jsp?test=<script>alert\(document.domain\)</script>](http://server/tomcat-docs/appdev/sample/web/hello.jsp?test=<script>alert(document.domain)</script>)

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1355>
CVE-2007-1355

ADDITIONAL INFORMATION

The information has been provided by <mailto:markt@xxxxxxxxxx> Mark Thomas.

The original article can be found at:
<http://tomcat.apache.org/security-6.html>
<http://tomcat.apache.org/security-6.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.