

[VulnWatch] wp-02-0008: Apache Tomcat Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0018.html>

From: Matt Moore (matt@westpoint.ltd.uk)

Date: 07/10/02

Date: Wed, 10 Jul 2002 12:09:18 +0100
From: Matt Moore <matt@westpoint.ltd.uk>
To: vulnwatch@vulnwatch.org

Westpoint Security Advisory

Title: Apache Tomcat Cross Site Scripting

Risk Rating: Low

Software: Apache Tomcat v4.0.3

Platforms: WinNT, Win2k, Linux

Vendor URL: jakarta.apache.org

Author: Matt Moore <matt@westpoint.ltd.uk>

Date: 10th July 2002

Advisory ID#: wp-02-0008

Overview:

=====

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:

=====

Cross Site Scripting

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
```

VulnWatch: [VulnWatch] wp-02-0008: Apache Tomcat Cross Site Scripting

Linux and Win32 versions of Tomcat are vulnerable.

(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)"
```

This is obviously Win32 specific.

Vendor Response:

=====

None.

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.

Two Nessus plugins should be available to test for these vulnerabilities from www.nessus.org:

```
apache_tomcat_DOS_Device_XSS.nasl  
apache_tomcat_Servlet_XSS.nasl
```

This advisory is available online at:

<http://www.westpoint.ltd.uk/advisories/wp-02-0008.txt>

- **Previous message:** [Matt Moore: "\[VulnWatch\] wp-02-0001: GoAhead Web Server Directory Traversal + Cross Site Scripting"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)