



CVE-2005-4838

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 02/13/2023 02:16:00 AM UTC

CVE-2005-4838

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Tomcat](#) from [Apache](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the example web applications for Jakarta Tomcat 5.5.6 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) `el/functions.jsp`, (2) `el/implicit-objects.jsp`, and (3) `jspx/textRotate.jsp` in `examples/jsp2/`, as demonstrated via script in a request to

`snp/snoop.jsp`. NOTE: other XSS issues in the manager were simultaneously reported, but these require admin access and do not cross privilege boundaries.

CVE-2005-4838 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Pony Mail!

[lists.apache.org](#)
[text/html](#)

MLIST [tomcat-dev] 20190319 svn commit: r1855831 [21/30] - in /tomcat/site/trunk: ./ docs/ xdocs/

No Description Provided

[www.osvdb.org](#)

OSVDB 34878

Inactive Link Not Archived

[www.oliverkarow.de](#)
[text/plain](#)

MISC
www.oliverkarow.de/research/jakarta556_xss.txt

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

XF tomcat-functions-xss(36467)

	text/html	
Secunia - Advisories - Apache Tomcat "Tomcat Manager" Cross-Site Scripting	Patch Vendor Advisory web.archive.org text/html	SECUNIA 13737
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0261
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 12721
[Full-disclosure] Apache Tomcat remote xss	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20070906 Apache Tomcat remote xss
Pony Mail!	lists.apache.org text/html	MLIST [tomcat-dev] 20200213 svn commit: r1873980 [24/34] - /tomcat/site/trunk/docs/
No Description Provided	marc.info text/html	MLIST [tomcat-dev] 20050103 Re: Fwd: XSS in Jakarta Tomcat 5.5.6
Pony Mail!	lists.apache.org text/html	MLIST [tomcat-dev] 20190325 svn commit: r1856174 [19/29] - in /tomcat/site/trunk: docs/ xdocs/ xdocs/stylesheets/
Red Hat update for Red Hat Network Satellite Server - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 31493
Apache Tomcat® - Apache Tomcat 4.x vulnerabilities	tomcat.apache.org text/xml	CONFIRM tomcat.apache.org/security-4.html
access.redhat.com	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2008:0630
Apache Tomcat - Apache Tomcat 5 vulnerabilities	tomcat.apache.org text/html	CONFIRM tomcat.apache.org/security-5.html
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 34879
SecurityTracker.com Archives - Jakarta Tomcat Manager Input Validation Holes Permit Cross-Site Scripting Attacks	securitytracker.com text/html	SECTRAK 1012793
'[PATCH jakarta-servletapi-5] Re: Fwd: XSS in Jakarta Tomcat 5.5.6' - MARC	marc.info text/html	MLIST [tomcat-dev] 20050103 [PATCH jakarta-servletapi-5] Re: Fwd: XSS in Jakarta Tomcat 5.5.6

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
A	I	T	A	A	A	A

Application	Apache	Tomcat	All	All	All	All
cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID						Next ID →

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report