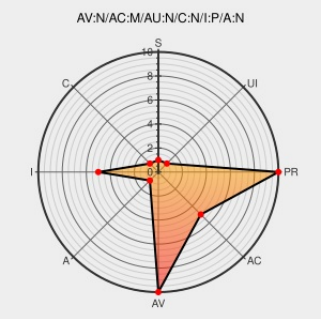
CVE-2005-4838

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.jspx 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 Inactive Link Not Archived	OSVDB 34878
	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
rhn.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	SECTRACK 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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

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→