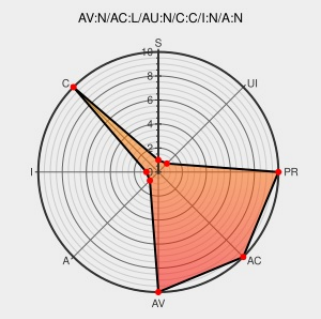
CVE-2005-4836

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

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4836

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tomcat from Apache contain the following vulnerability:

The HTTP/1.1 connector in Apache Tomcat 4.1.15 through 4.1.40 does not reject NULL bytes in a URL when allowLinking is configured, which allows remote attackers to read JSP source files and obtain sensitive information.

CVE-2005-4836 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	NONE

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [tomcat-dev] 20190325 svn commit: r1856174 [19/29] - in /tomcat/site/trunk: docs/ xdocs/ xdocs/stylesheets/
Pony Mail!	lists.apache.org text/html	MLIST [tomcat-dev] 20190319 svn commit: r1855831 [21/30] - in /tomcat/site/trunk: ./ docs/ xdocs/
Pony Mail!	lists.apache.org text/html	MLIST [tomcat-dev] 20200213 svn commit: r1873980 [24/34] - /tomcat/site/trunk/docs/
Apache Tomcat® - Apache Tomcat 4.x vulnerabilities	tomcat.apache.org text/xml	CONFIRM tomcat.apache.org/security-4.html
Apache Tomcat 'allowLinking' Accepts NULL Byte in URI Information Disclosure Vulnerability	cve.report (archive) text/html	BID 28483

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.

Related QID Numbers

995384 Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-qrcx-p4rr-g48h)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	4.1.15	All	All	All
Application	Apache	Tomcat	4.1.16	All	All	All
Application	Apache	Tomcat	4.1.17	All	All	All
Application	Apache	Tomcat	4.1.18	All	All	All
Application	Apache	Tomcat	4.1.19	All	All	All
Application	Apache	Tomcat	4.1.20	All	All	All
Application	Apache	Tomcat	4.1.21	All	All	All
Application	Apache	Tomcat	4.1.22	All	All	All
Application	Apache	Tomcat	4.1.23	All	All	All
Application	Apache	Tomcat	4.1.24	All	All	All
Application	Apache	Tomcat	4.1.25	All	All	All
Application	Apache	Tomcat	4.1.26	All	All	All
Application	Apache	Tomcat	4.1.27	All	All	All
Application	Apache	Tomcat	4.1.28	alpha	All	All
Application	Apache	Tomcat	4.1.29	All	All	All
Application	Apache	Tomcat	4.1.29	alpha	All	All
Application	Apache	Tomcat	4.1.30	All	All	All
Application	Apache	Tomcat	4.1.31	All	All	All
Application	Apache	Tomcat	4.1.32	All	All	All
Application	Apache	Tomcat	4.1.33	All	All	All
Application	Apache	Tomcat	4.1.34	All	All	All
Application	Apache	Tomcat	4.1.35	All	All	All
Application	Apache	Tomcat	4.1.36	All	All	All
Application	Apache	Tomcat	4.1.37	All	All	All
Application	Apache	Tomcat	4.1.39	All	All	All
Application	Apache	Tomcat	4.1.40	All	All	All
Application	Apache	Tomcat	4.1.15	All	All	All
Application	Apache	Tomcat	4.1.16	All	All	All

Application	Apache	Tomcat	4.1.17	All	All	All
Application	Apache	Tomcat	4.1.18	All	All	All
Application	Apache	Tomcat	4.1.19	All	All	All
Application	Apache	Tomcat	4.1.20	All	All	All
Application	Apache	Tomcat	4.1.21	All	All	All
Application	Apache	Tomcat	4.1.22	All	All	All
Application	Apache	Tomcat	4.1.23	All	All	All
Application	Apache	Tomcat	4.1.24	All	All	All
Application	Apache	Tomcat	4.1.25	All	All	All
Application	Apache	Tomcat	4.1.26	All	All	All
Application	Apache	Tomcat	4.1.27	All	All	All
Application	Apache	Tomcat	4.1.28	alpha	All	All
Application	Apache	Tomcat	4.1.29	All	All	All
Application	Apache	Tomcat	4.1.29	alpha	All	All
Application	Apache	Tomcat	4.1.30	All	All	All
Application	Apache	Tomcat	4.1.31	All	All	All
Application	Apache	Tomcat	4.1.32	All	All	All
Application	Apache	Tomcat	4.1.33	All	All	All
Application	Apache	Tomcat	4.1.34	All	All	All
Application	Apache	Tomcat	4.1.35	All	All	All
Application	Apache	Tomcat	4.1.36	All	All	All
Application	Apache	Tomcat	4.1.37	All	All	All
Application	Apache	Tomcat	4.1.39	All	All	All
Application	Apache	Tomcat	4.1.40	All	All	All

cpe:2.3:a:apache:tomcat:4.1.15:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.16:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.17:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.18:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.19:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.20:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.21:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.22:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.23:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.24:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.25:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.26:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.27:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.28:alpha:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.29:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.29:alpha:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.30:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.31:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.32:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.33:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.34:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.35:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.36:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.37:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.39:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.40:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.15:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.16:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.17:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.18:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.19:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.20:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.21:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.22:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.23:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.24:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.25:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.26:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.26:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.27:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.28:alpha:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.29:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.29:alpha:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.30:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.31:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.32:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.33:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.34:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.35:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.36:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.37:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.39:*:*:*:*:*:*:*

cpe:2.3:a:apache:tomcat:4.1.40:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→