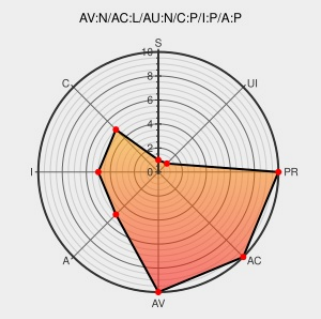
CVE-2002-1394

Published on: 01/17/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1394

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



Certain versions of Tomcat from Apache contain the following vulnerability:

Apache Tomcat 4.0.5 and earlier, when using both the invoker servlet and the default servlet, allows remote attackers to read source code for server files or bypass certain protections, a variant of CAN-2002-1148.

CVE-2002-1394 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
'GLSA: tomcat' - MARC	marc.info text/html	GENTOO GLSA-200210-001
Support	www.redhat.com text/html	REDHAT RHSA-2003:075
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tomcat-invoker-source-code(10376)
Debian -- Security Information -- DSA-225-1 tomcat4	www.debian.org Depreciated Link text/html	DEBIAN DSA-225
Apache Tomcat Invoker Servlet File Disclosure Vulnerability	cve.report (archive) text/html	BID 6562
Pony Mail!	lists.apache.org	MLIST [tomcat-dev] 20190325 svn commit:

	text/html	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/
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:082
'[SECURITY] Apache Tomcat 4.x JSP source disclosure vulnerability;' - MARC	marc.info text/html	CONFIRM marc.info/?l=tomcat-dev&m=103417249325526&w=2
Bug 13365 - JSP source disclosure vulnerability not fixed when invoking servlets by name	issues.apache.org text/html	CONFIRM issues.apache.org/bugzilla/show_bug.cgi?id=13365

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	4.0.0	All	All	All
Application	Apache	Tomcat	4.0.1	All	All	All
Application	Apache	Tomcat	4.0.2	All	All	All
Application	Apache	Tomcat	4.0.3	All	All	All
Application	Apache	Tomcat	4.0.4	All	All	All
Application	Apache	Tomcat	4.0.5	All	All	All
Application	Apache	Tomcat	4.1.0	All	All	All
Application	Apache	Tomcat	4.1.10	All	All	All
Application	Apache	Tomcat	4.1.3	beta	All	All
Application	Apache	Tomcat	4.1.9	beta	All	All
Application	Apache	Tomcat	4.0.0	All	All	All
Application	Apache	Tomcat	4.0.1	All	All	All
Application	Apache	Tomcat	4.0.2	All	All	All
Application	Apache	Tomcat	4.0.3	All	All	All
Application	Apache	Tomcat	4.0.4	All	All	All
Application	Apache	Tomcat	4.0.5	All	All	All
Application	Apache	Tomcat	4.1.0	All	All	All
Application	Apache	Tomcat	4.1.10	All	All	All
Application	Apache	Tomcat	4.1.3	beta	All	All

Application	Apache	Tomcat	4.1.3	beta	All	All
Application	Apache	Tomcat	4.1.9	beta	All	All

cpe:2.3:a:apache:tomcat:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.10:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.3:beta:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.9:beta:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.10:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.3:beta:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:4.1.9:beta:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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