



CVE-2008-2370

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-2370
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-04 01:41:00 UTC
Updated	2023-02-13 02:19:00 UTC
Description	Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through 6.0.16, when a RequestDispatcher is used, p

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	4.1.0	All	All	All
Application	Apache	Tomcat	4.1.1	All	All	All
Application	Apache	Tomcat	4.1.10	All	All	All
Application	Apache	Tomcat	4.1.11	All	All	All
Application	Apache	Tomcat	4.1.12	All	All	All
Application	Apache	Tomcat	4.1.13	All	All	All
Application	Apache	Tomcat	4.1.14	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	4.1.2	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	All	All	All
Application	Apache	Tomcat	4.1.29	All	All	All
Application	Apache	Tomcat	4.1.3	All	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	4.1.4	All	All	All
Application	Apache	Tomcat	4.1.5	All	All	All
Application	Apache	Tomcat	4.1.6	All	All	All
Application	Apache	Tomcat	4.1.7	All	All	All
Application	Apache	Tomcat	4.1.8	All	All	All
Application	Apache	Tomcat	4.1.9	All	All	All
Application	Apache	Tomcat	5.5.0	All	All	All
Application	Apache	Tomcat	5.5.1	All	All	All
Application	Apache	Tomcat	5.5.10	All	All	All
Application	Apache	Tomcat	5.5.11	All	All	All
Application	Apache	Tomcat	5.5.12	All	All	All
Application	Apache	Tomcat	5.5.13	All	All	All
Application	Apache	Tomcat	5.5.14	All	All	All
Application	Apache	Tomcat	5.5.15	All	All	All
Application	Apache	Tomcat	5.5.16	All	All	All
Application	Apache	Tomcat	5.5.17	All	All	All
Application	Apache	Tomcat	5.5.18	All	All	All
Application	Apache	Tomcat	5.5.19	All	All	All
Application	Apache	Tomcat	5.5.2	All	All	All
Application	Apache	Tomcat	5.5.20	All	All	All

Application	Apache	Tomcat	5.5.21	All	All	All
Application	Apache	Tomcat	5.5.22	All	All	All
Application	Apache	Tomcat	5.5.23	All	All	All
Application	Apache	Tomcat	5.5.24	All	All	All
Application	Apache	Tomcat	5.5.25	All	All	All
Application	Apache	Tomcat	5.5.26	All	All	All
Application	Apache	Tomcat	5.5.3	All	All	All
Application	Apache	Tomcat	5.5.4	All	All	All
Application	Apache	Tomcat	5.5.5	All	All	All
Application	Apache	Tomcat	5.5.6	All	All	All
Application	Apache	Tomcat	5.5.7	All	All	All
Application	Apache	Tomcat	5.5.8	All	All	All
Application	Apache	Tomcat	5.5.9	All	All	All
Application	Apache	Tomcat	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.10	All	All	All
Application	Apache	Tomcat	6.0.11	All	All	All
Application	Apache	Tomcat	6.0.12	All	All	All
Application	Apache	Tomcat	6.0.13	All	All	All
Application	Apache	Tomcat	6.0.14	All	All	All
Application	Apache	Tomcat	6.0.15	All	All	All
Application	Apache	Tomcat	6.0.16	All	All	All
Application	Apache	Tomcat	6.0.2	All	All	All
Application	Apache	Tomcat	6.0.3	All	All	All
Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.5	All	All	All
Application	Apache	Tomcat	6.0.6	All	All	All
Application	Apache	Tomcat	6.0.7	All	All	All
Application	Apache	Tomcat	6.0.8	All	All	All
Application	Apache	Tomcat	6.0.9	All	All	All
Application	Apache	Tomcat	4.1.0	All	All	All
Application	Apache	Tomcat	4.1.1	All	All	All
Application	Apache	Tomcat	4.1.10	All	All	All
Application	Apache	Tomcat	4.1.11	All	All	All
Application	Apache	Tomcat	4.1.12	All	All	All
Application	Apache	Tomcat	4.1.13	All	All	All

Application	Apache	Tomcat	4.1.13	All	All	All
Application	Apache	Tomcat	4.1.14	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	4.1.2	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	All	All	All
Application	Apache	Tomcat	4.1.29	All	All	All
Application	Apache	Tomcat	4.1.3	All	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	4.1.4	All	All	All
Application	Apache	Tomcat	4.1.5	All	All	All
Application	Apache	Tomcat	4.1.6	All	All	All
Application	Apache	Tomcat	4.1.7	All	All	All
Application	Apache	Tomcat	4.1.8	All	All	All
Application	Apache	Tomcat	4.1.9	All	All	All
Application	Apache	Tomcat	5.5.0	All	All	All
Application	Apache	Tomcat	5.5.1	All	All	All
Application	Apache	Tomcat	5.5.10	All	All	All

Application	Apache	Tomcat	5.5.11	All	All	All
Application	Apache	Tomcat	5.5.12	All	All	All
Application	Apache	Tomcat	5.5.13	All	All	All
Application	Apache	Tomcat	5.5.14	All	All	All
Application	Apache	Tomcat	5.5.15	All	All	All
Application	Apache	Tomcat	5.5.16	All	All	All
Application	Apache	Tomcat	5.5.17	All	All	All
Application	Apache	Tomcat	5.5.18	All	All	All
Application	Apache	Tomcat	5.5.19	All	All	All
Application	Apache	Tomcat	5.5.2	All	All	All
Application	Apache	Tomcat	5.5.20	All	All	All
Application	Apache	Tomcat	5.5.21	All	All	All
Application	Apache	Tomcat	5.5.22	All	All	All
Application	Apache	Tomcat	5.5.23	All	All	All
Application	Apache	Tomcat	5.5.24	All	All	All
Application	Apache	Tomcat	5.5.25	All	All	All
Application	Apache	Tomcat	5.5.26	All	All	All
Application	Apache	Tomcat	5.5.3	All	All	All
Application	Apache	Tomcat	5.5.4	All	All	All
Application	Apache	Tomcat	5.5.5	All	All	All
Application	Apache	Tomcat	5.5.6	All	All	All
Application	Apache	Tomcat	5.5.7	All	All	All
Application	Apache	Tomcat	5.5.8	All	All	All
Application	Apache	Tomcat	5.5.9	All	All	All
Application	Apache	Tomcat	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.10	All	All	All
Application	Apache	Tomcat	6.0.11	All	All	All
Application	Apache	Tomcat	6.0.12	All	All	All
Application	Apache	Tomcat	6.0.13	All	All	All
Application	Apache	Tomcat	6.0.14	All	All	All
Application	Apache	Tomcat	6.0.15	All	All	All
Application	Apache	Tomcat	6.0.16	All	All	All
Application	Apache	Tomcat	6.0.2	All	All	All
Application	Apache	Tomcat	6.0.3	All	All	All

Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.5	All	All	All
Application	Apache	Tomcat	6.0.6	All	All	All
Application	Apache	Tomcat	6.0.7	All	All	All
Application	Apache	Tomcat	6.0.8	All	All	All
Application	Apache	Tomcat	6.0.9	All	All	All

References						
Reference				Source		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN		
Apache Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA		
Pony Mail!				MISC		
Pony Mail!				MISC		
Security Advisories Mandriva Linux				MANDRIVA		
IBM X-Force Exchange				XF		
Repository / Oval Repository				OVAL		
Apache Tomcat 'RequestDispatcher' Information Disclosure Vulnerability				BID		
SecurityReason - Apache Tomcat information disclosure vulnerability				SREASON		
VMware Products Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA		
About Secunia Research Flexera				SECUNIA		
Pony Mail!				MLIST		
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:018				SUSE		
SecurityTracker: Tomcat RequestDispatcher Bug Lets Remote Users Bypass Access Restrictions				SECURITY		
This page provides Security Information. : Fujitsu Global				CONFIDENTIAL		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN		
ASA-2008-401 (RHSA-2008-0862)				CONFIDENTIAL		
Red Hat update for tomcat - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA		
access.redhat.com				REDHAT		
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA		
HP-UX update for Apache - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA		
SecurityFocus				BUGTRAQ		
[SECURITY] Fedora 8 Update: tomcat5-5.5.27-0jpp.2.fc8				FEDORA		
Pony Mail!				MISC		
VMSA-2009-0002 - VMware				CONFIDENTIAL		
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA		
RETIRED: Apple Mac OS X 2008-007 Multiple Security Vulnerabilities				BID		

Pony Mail!	MLIST
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
access.redhat.com	REDHA
About Security Update 2008-007	CONFIF
Fedora update for tomcat6 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUN
Pony Mail!	MLIST
VMware Multiple Products Tomcat Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
Pony Mail!	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Pony Mail!	MLIST
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Pony Mail!	MISC
Apache Tomcat® - Apache Tomcat 4.x vulnerabilities	CONFIF
access.redhat.com	REDHA
Apache Tomcat - Apache Tomcat 5 vulnerabilities	CONFIF
APPLE-SA-2008-10-09 Security Update 2008-007	APPLE
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:004	SUSE
Pony Mail!	MISC
[SECURITY] Fedora 9 Update: tomcat6-6.0.18-1.1.fc9	FEDOR
Pony Mail!	MLIST
Avaya AES / MX Apache Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUN
[SECURITY] Fedora 9 Update: tomcat5-5.5.27-0jpp.2.fc9	FEDOR
Apache ODE Process Deployment Web Service Directory Traversal - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
SecurityFocus	BUGTR
Pony Mail!	MISC
Pony Mail!	MLIST
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
VMware VirtualCenter update for Tomcat - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
Fedora update for tomcat5 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
VMSA-2009-0016.1	CONFIF
Fujitsu Interstage Products Information Disclosure Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
HPSBUX02401	HP
Apache Tomcat 6 Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUN

'[security bulletin] HPSBST02955 rev.1 - HP XP P9000 Performance Advisor Software, 3rd party Software' - MARC	HP
Red Hat update for tomcat - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUN
Repository / Oval Repository	OVAL
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	CONFIF
Pony Mail!	MLIST
CVE Program record	CVE.OF
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

997496 Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-m8h8-6rvg-f4mg)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)