



CVE-2010-4172

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

Summary

CVE	CVE-2010-4172
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-26 20:00:00 UTC
Updated	2023-02-13 04:28:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Manager application in Apache Tomcat 6.0.12 through 6.0.29 and 7.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	6.0.17	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All
Application	Apache	Tomcat	6.0.19	All	All	All
Application	Apache	Tomcat	6.0.20	All	All	All
Application	Apache	Tomcat	6.0.24	All	All	All
Application	Apache	Tomcat	6.0.26	All	All	All
Application	Apache	Tomcat	6.0.27	All	All	All
Application	Apache	Tomcat	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	7.0.0	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.1	All	All	All

Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All
Application	Apache	Tomcat	7.0.4	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	6.0.17	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All
Application	Apache	Tomcat	6.0.19	All	All	All
Application	Apache	Tomcat	6.0.20	All	All	All
Application	Apache	Tomcat	6.0.24	All	All	All
Application	Apache	Tomcat	6.0.26	All	All	All
Application	Apache	Tomcat	6.0.27	All	All	All
Application	Apache	Tomcat	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	7.0.0	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.1	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All

References						
Reference	Source					
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC					
Red Hat Customer Portal	MISC					
[Apache-SVN] Revision 1037779	CONF					
About Secunia Research Flexera	SEC					
Red Hat Customer Portal	RED					
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FULL					
Red Hat Customer Portal	MISC					
Bug 656246 – CVE-2010-4172 tomcat: cross-site-scripting vulnerability in the manager application	CONF					
Red Hat Customer Portal	RED					

Security racker.com Archives - Apache Tomcat Manager Input Validation Hole in 'sessionList.jsp' Permits Cross-Site Scripting Attacks	SEC
Novell Sentinel Log Manager Java and Tomcat Vulnerabilities - Secunia.com	SEC
SecurityFocus	BUG
Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities	BID
Red Hat Customer Portal	RED
APPLE-SA-2011-10-12-3 OS X Lion v10.7.2 and Security Update 2011-006	APP
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUP
USN-1048-1: Tomcat vulnerability Ubuntu	UBU
About the security content of OS X Lion v10.7.2 and Security Update 2011-006	COM
CVE-2010-4172 - Red Hat Customer Portal	MISC
Ubuntu update for tomcat6 - Advisories - Community	SEC
Apache Tomcat® - Apache Tomcat 7 vulnerabilities	COM
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUP
Apache Tomcat Manager "sort" and "orderBy" Cross-Site Scripting Vulnerabilities - Advisories - Community	SEC
Sentinel Log Manager 1.2.0.1 (1.2 Hot Fix 1)	COM
'[security bulletin] HPSBST02955 rev.1 - HP XP P9000 Performance Advisor Software, 3rd party Software' - MARC	HP
[Apache-SVN] Revision 1037778	COM
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	COM
CVE Program record	CVE
NVD vulnerability detail	NVD
	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)