



CVE-2009-0781

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

Summary

CVE	CVE-2009-0781
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-09 21:30:00 UTC
Updated	2023-02-13 02:19:00 UTC
Description	Cross-site scripting (XSS) vulnerability in jsp/cal/cal2.jsp in the calendar application in the examples web application in Apache Tomcat 4.1.0 through 4.1.22. An attacker can inject arbitrary HTML and JavaScript code into the calendar application, which is then rendered by the browser. This can lead to session hijacking, account takeover, and other malicious actions. The vulnerability is caused by the lack of proper output encoding in the jsp/cal/cal2.jsp file.

Risk And Classification

Problem Types: CWE-79

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	4.1.3	beta	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	4.1.9	beta	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	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	4.1.10	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	4.1.3	beta	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	4.1.9	beta	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	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	List	
Pony Mail!				MISC	list	
Pony Mail!				MISC	list	
'[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC				HP	ma	
IBM X-Force Exchange				XF	ex	
Repository / Oval Repository				OVAL	ov	
Security Advisories Mandriva Linux				MANDRIVA	wv	
VMware Products Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA	se	
Pony Mail!				MLIST	list	
'[security bulletin] HPSBUX02579 SSRT100203 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC				HP	ma	
Repository / Oval Repository				OVAL	ov	
Red Hat Customer Portal				MISC	ac	
263529				SUNALERT	su	
SecurityFocus				BUGTRAQ	wv	
SecurityFocus				BUGTRAQ	wv	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	wv	
Pony Mail!				MISC	list	
[SECURITY] Fedora 11 Update: tomcat6-6.0.20-1.fc11				FEDORA	wv	
Pony Mail!				MLIST	list	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	wv	
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3				APPLE	list	
[SECURITY] Fedora 10 Update: tomcat6-6.0.20-1.fc10				FEDORA	wv	

Pony Mail!	MLIST	list
Pony Mail!	MISC	list
Repository / Oval Repository	OVAL	ov
Pony Mail!	MLIST	list
Pony Mail!	MISC	list
Debian -- Security Information -- DSA-2207-1 tomcat5.5	DEBIAN	wv
Apache Tomcat® - Apache Tomcat 4.x vulnerabilities	CONFIRM	tor
Apache Tomcat - Apache Tomcat 5 vulnerabilities	CONFIRM	tor
Pony Mail!	MISC	list
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	se
Pony Mail!	MLIST	list
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:012	SUSE	list
Pony Mail!	MISC	list
489028 – (CVE-2009-0781) CVE-2009-0781 tomcat: XSS in Apache Tomcat calendar application	MISC	bu
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	wv
[SECURITY] Fedora 12 Update: tomcat6-6.0.20-1.fc12	FEDORA	wv
Pony Mail!	MLIST	list
Sun Solaris Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	se
Security Advisories Mandriva Linux	MANDRIVA	wv
VMSA-2009-0016.1	CONFIRM	wv
HP-UX update for Tomcat Servlet Engine - Advisories - Community	SECUNIA	se
Red Hat Customer Portal	MISC	ac
CVE-2009-0781 - Red Hat Customer Portal	MISC	ac
'[security bulletin] HPSBOV02762 SSRT100825 rev.1 - HP Secure Web Server (SWS) for OpenVMS running CS' - MARC	HP	ma
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	CONFIRM	su
'[security bulletin] HPSBMA02535 SSRT100029 rev.1 - HP Performance Manager, Remote Unauthorized Acces' - MARC	HP	ma
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	CONFIRM	tor
Pony Mail!	MLIST	list
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-03-17	Tomas Hoger	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com



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](#)