CVE-2007-2449

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-2449
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-14 23:30:00 UTC
Updated	2023-11-07 02:00:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in certain JSP files in the examples web application in Apache Tomcat 4.0.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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	5.0.0	All	All	All
Application	Apache	Tomcat	5.0.1	All	All	All
Application	Apache	Tomcat	5.0.10	All	All	All
Application	Apache	Tomcat	5.0.11	All	All	All
Application	Apache	Tomcat	5.0.12	All	All	All
Application	Apache	Tomcat	5.0.13	All	All	All
Application	Apache	Tomcat	5.0.14	All	All	All
Application	Apache	Tomcat	5.0.15	All	All	All
Application	Apache	Tomcat	5.0.16	All	All	All
Application	Apache	Tomcat	5.0.17	All	All	All
Application	Apache	Tomcat	5.0.18	All	All	All

Application	Apache	Tomcat	5.0.19	All	All	All
Application	Apache	Tomcat	5.0.2	All	All	All
Application	Apache	Tomcat	5.0.21	All	All	All
Application	Apache	Tomcat	5.0.22	All	All	All
Application	Apache	Tomcat	5.0.23	All	All	All
Application	Apache	Tomcat	5.0.24	All	All	All
Application	Apache	Tomcat	5.0.25	All	All	All
Application	Apache	Tomcat	5.0.26	All	All	All
Application	Apache	Tomcat	5.0.27	All	All	All
Application	Apache	Tomcat	5.0.28	All	All	All
Application	Apache	Tomcat	5.0.29	All	All	All
Application	Apache	Tomcat	5.0.3	All	All	All
Application	Apache	Tomcat	5.0.30	All	All	All
Application	Apache	Tomcat	5.0.4	All	All	All
Application	Apache	Tomcat	5.0.5	All	All	All
Application	Apache	Tomcat	5.0.6	All	All	All
Application	Apache	Tomcat	5.0.7	All	All	All
Application	Apache	Tomcat	5.0.8	All	All	All
Application	Apache	Tomcat	5.0.9	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	5.5.3	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	6.0.2	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	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	5.0.0	All	All	All
Application	Apache	Tomcat	5.0.1	All	All	All
Application	Apache	Tomcat	5.0.10	All	All	All
Application	Apache	Tomcat	5.0.11	All	All	All
Application	Apache	Tomcat	5.0.12	All	All	All
Application	Apache	Tomcat	5.0.13	All	All	All
Application	Apache	Tomcat	5.0.14	All	All	All
Application	Apache	Tomcat	5.0.15	All	All	All
Application	Apache	Tomcat	5.0.16	All	All	All

Application	Apache	Tomcat	5.0.17	All	All	All
Application	Apache	Tomcat	5.0.18	All	All	All
Application	Apache	Tomcat	5.0.19	All	All	All
Application	Apache	Tomcat	5.0.2	All	All	All
Application	Apache	Tomcat	5.0.21	All	All	All
Application	Apache	Tomcat	5.0.22	All	All	All
Application	Apache	Tomcat	5.0.23	All	All	All
Application	Apache	Tomcat	5.0.24	All	All	All
Application	Apache	Tomcat	5.0.25	All	All	All
Application	Apache	Tomcat	5.0.26	All	All	All
Application	Apache	Tomcat	5.0.27	All	All	All
Application	Apache	Tomcat	5.0.28	All	All	All
Application	Apache	Tomcat	5.0.29	All	All	All
Application	Apache	Tomcat	5.0.3	All	All	All
Application	Apache	Tomcat	5.0.30	All	All	All
Application	Apache	Tomcat	5.0.4	All	All	All
Application	Apache	Tomcat	5.0.5	All	All	All
Application	Apache	Tomcat	5.0.6	All	All	All
Application	Apache	Tomcat	5.0.7	All	All	All
Application	Apache	Tomcat	5.0.8	All	All	All
Application	Apache	Tomcat	5.0.9	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	5.5.3	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	6.0.2	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	All	All	All	All

References

Reference
Apache Tomcat JSP Example Web Applications Cross Site Scripting Vulnerability
Friday, January 23, 2009 - Posts - CA Security Response Blog - CA Technologies
rhn.redhat.com | Red Hat Support
About the security content of Security Update 2008-004 and Mac OS X 10.5.4
SecurityFocus
SecurityFocus
Repository / Oval Repository
IBM X-Force Exchange
rhn.redhat.com | Red Hat Support
[security-announce] SUSE Security Summary Report SUSE-SR:2008:007
404 Not Found

404 Not Found

Pony Mail!

SecurityReason - Apache Tomcat XSS vulnerabilities in the JSP examples

Fedora update for tomcat5 - Advisories - Secunia

APPLE-SA-2008-06-30 Security Update 2008-004 and Mac OS X v10.5.4

Advisories | Mandriva

Pony Mail!

Pony Mail!

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Pony Mail!

[SECURITY] Fedora 7 Update: tomcat5-5.5.25-1jpp.1.fc7

SecurityTracker.com Archives - Tomcat Input Validation Holes in the JSP Examples, Manager, and Host Manager Permit Cross-Site Scripting

Pony Mail!

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat update for Red Hat Network Satellite Server - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Apache Tomcat® - Apache Tomcat 4.x vulnerabilities

access.redhat.com

Apache Tomcat - Apache Tomcat 5 vulnerabilities

[security-announce] SUSE Security Summary Report: SUSE-SR:2009:004

Pony Mail!

36080

SUSE Update for Multiple Packages - Advisories - Secunia

HP-UX update for Apache - Advisories - Secunia

Pony Mail!

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityFocus

HPSBUX02262 SSRT071447 rev. 1 - HP-UX running Apache, Remote Arbitrary Code Execution, Cross Site Scripting (XSS) - c01178795 - HP

Pony Mail!

Red Hat update for tomcat - Advisories - Secunia

CA Cohesion Application Configuration Manager Apache Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Sec

Pony Mail!

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Apache Tomcat® - Apache Tomcat 6 vulnerabilities

Pony Mail!

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995375 Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-hc39-rjwp-qffq)