



CVE-2009-0580

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

Summary

CVE	CVE-2009-0580
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-05 16:00:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when FORM authentication is used, a

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:N/A:N

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

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	4.1.38	All	All	All
Application	Apache	Tomcat	4.1.39	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	5.5.27	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

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference						Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						af854a3a-2127-4
'[security bulletin] HPSBUX02579 SSRT100203 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC						af854a3a-2127-4
Apache Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com						af854a3a-2127-4
VMware Products Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com						af854a3a-2127-4
Debian -- Security Information -- DSA-2207-1 tomcat5.5						af854a3a-2127-4
'[security bulletin] HPSBMA02535 SSRT100029 rev.1 - HP Performance Manager, Remote Unauthorized Acces' - MARC						af854a3a-2127-4
Pony Mail!						af854a3a-2127-4
Repository / Oval Repository						af854a3a-2127-4
Apache Tomcat® - Apache Tomcat 4.x vulnerabilities						af854a3a-2127-4
[Apache-SVN] Revision 747840						af854a3a-2127-4
HP-UX update for Tomcat Servlet Engine - Advisories - Community						af854a3a-2127-4
Security Advisories Mandriva Linux						af854a3a-2127-4
[SECURITY] Fedora 11 Update: tomcat6-6.0.20-1.fc11						af854a3a-2127-4
[SECURITY] Fedora 10 Update: tomcat6-6.0.20-1.fc10						af854a3a-2127-4

Pony Mail!	af854a3a-2127-4
SecurityTracker.com Archives - Tomcat Authentication Response Error Lets Remote Users Determine Valid Usernames	af854a3a-2127-4
'[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
Security Advisories Mandriva Linux	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
Apache Tomcat Form Authentication Existing/Non-Existing Username Enumeration Weakness	af854a3a-2127-4
IBM X-Force Exchange	af854a3a-2127-4
Sun Solaris Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-4
Repository / Oval Repository	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
[SECURITY] Fedora 12 Update: tomcat6-6.0.20-1.fc12	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	af854a3a-2127-4
Apache Tomcat - Apache Tomcat 5 vulnerabilities	af854a3a-2127-4
[Apache-SVN] Revision 781382	af854a3a-2127-4
Pony Mail!	af854a3a-2127-4
[Apache-SVN] Revision 781379	af854a3a-2127-4
sunsolve.sun.com/search/document.do	af854a3a-2127-4
Pony Mail!	af854a3a-2127-4
Security Advisories Mandriva Linux	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
Apache Tomcat 6 Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-4
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	af854a3a-2127-4
Pony Mail!	af854a3a-2127-4
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	af854a3a-2127-4
VMSA-2009-0016.1	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
'[security bulletin] HPSBOV02762 SSRT100825 rev.1 - HP Secure Web Server (SWS) for OpenVMS running CS' - MARC	af854a3a-2127-4
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-4
Pony Mail!	af854a3a-2127-4
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:012	af854a3a-2127-4
Repository / Oval Repository	af854a3a-2127-4
Pony Mail!	af854a3a-2127-4
Pony Mail!	MITRE

Vendor Name	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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