



CVE-2010-1157

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

Summary

CVE	CVE-2010-1157
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-04-23 14:30:00 UTC
Updated	2023-02-13 04:17:00 UTC
Description	Apache Tomcat 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 might allow remote attackers to discover the server's hostname

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	5.5.28	All	All	All
Application	Apache	Tomcat	5.5.29	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	6.0.17	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All
Application	Apache	Tomcat	6.0.19	All	All	All
Application	Apache	Tomcat	6.0.2	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	6.0.3	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	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	5.5.28	All	All	All
Application	Apache	Tomcat	5.5.29	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	6.0.12	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	6.0.2	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	6.0.3	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	Link
Pony Mail!	MISC	list
'[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	HP	ma
Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability	BID	ww
About Secunia Research Flexera	SECUNIA	se
Pony Mail!	MLIST	list
'[security bulletin] HPSBUX02579 SSRT100203 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	HP	ma
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:017	SUSE	list
SecurityFocus	BUGTRAQ	ww
VMSA-2011-0003	CONFIRM	ww
Red Hat Customer Portal	REDHAT	ww
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Pony Mail!	MISC	list
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Pony Mail!	MISC	list

Debian -- Security Information -- DSA-2207-1 tomcat5.5	DEBIAN	www
Red Hat Customer Portal	REDHAT	www
APPLE-SA-2011-10-12-3 OS X Lion v10.7.2 and Security Update 2011-006	APPLE	list
Apache Tomcat - Apache Tomcat 5 vulnerabilities	CONFIRM	tor
Security Advisories Mandriva Linux	MANDRIVA	ww
Apache Tomcat Information Disclosure and Denial of Service - Advisories - Community	SECUNIA	se
VMware vCenter / ESX Server Apache Tomcat Multiple Vulnerabilities - Advisories - Community	SECUNIA	se
Security Advisories Mandriva Linux	MANDRIVA	ww
Pony Mail!	MLIST	list
About the security content of OS X Lion v10.7.2 and Security Update 2011-006	CONFIRM	su
Pony Mail!	MISC	list
[Apache-SVN] Revision 936540	CONFIRM	sv
Pony Mail!	MLIST	list
Repository / Oval Repository	OVAL	ov
HP-UX update for Tomcat Servlet Engine - Advisories - Community	SECUNIA	se
[Apache-SVN] Revision 936541	CONFIRM	sv
'[security bulletin] HPSBOV02762 SSRT100825 rev.1 - HP Secure Web Server (SWS) for OpenVMS running CS' - MARC	HP	ma
'[security bulletin] HPSBST02955 rev.1 - HP XP P9000 Performance Advisor Software, 3rd party Software' - MARC	HP	ma
VMware vCenter Server 4.1 Update 1 Release Notes	CONFIRM	ww
SecurityFocus	BUGTRAQ	ww
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	CONFIRM	tor
Pony Mail!	MLIST	list
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-07-13	Vincent Danen	For official statement, please refer to: https://www.redhat.com/security/data/cve/CVE-2010-11



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

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