CVE-2012-0022

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

Summary

CVE	CVE-2012-0022
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-01-19 04:01:16 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Apache Tomcat 5.5.x before 5.5.35, 6.x before 6.0.34, and 7.x before 7.0.23 uses an inefficient approach for handling para

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

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	5.5.30	All	All	All
Application	Apache	Tomcat	5.5.31	All	All	All
Application	Apache	Tomcat	5.5.32	All	All	All
Application	Apache	Tomcat	5.5.33	All	All	All
Application	Apache	Tomcat	5.5.34	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	6.0.17	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	6.0.27	All	All	All
Application	Apache	Tomcat	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	6.0.3	All	All	All
Application	Apache	Tomcat	6.0.30	All	All	All
Application	Apache	Tomcat	6.0.31	All	All	All
Application	Apache	Tomcat	6.0.32	All	All	All
Application	Apache	Tomcat	6.0.33	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	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	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.12	All	All	All

Application	Apache	Tomcat	7.0.13	All	All	All
Application	Apache	Tomcat	7.0.14	All	All	All
Application	Apache	Tomcat	7.0.15	All	All	All
Application	Apache	Tomcat	7.0.16	All	All	All
Application	Apache	Tomcat	7.0.17	All	All	All
Application	Apache	Tomcat	7.0.18	All	All	All
Application	Apache	Tomcat	7.0.19	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.20	All	All	All
Application	Apache	Tomcat	7.0.21	All	All	All
Application	Apache	Tomcat	7.0.22	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All
Application	Apache	Tomcat	7.0.5	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.7	All	All	All
Application	Apache	Tomcat	7.0.8	All	All	All
Application	Apache	Tomcat	7.0.9	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Repository / Oval Repository	af854a3a-2127
Debian -- Security Information -- DSA-2401-1 tomcat6	af854a3a-2127
'[security bulletin] HPSBMU02747 SSRT100771 rev.1 - HP OpenView Network Node Manager (OV NNM) Running' - MARC	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Apache Tomcat Parameter Handling Denial of Service Vulnerability	af854a3a-2127
Security Advisory SA48790 - Red Hat update for tomcat5 - Secunia	af854a3a-2127
Oracle Critical Patch Update - January 2013	af854a3a-2127
Pony Mail!	af854a3a-2127
www.mandriva.com	af854a3a-2127
'[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	af854a3a-2127

Repository / Oval Repository	af854a3a-2127
Apache Tomcat® - Apache Tomcat 7 vulnerabilities	af854a3a-2127
IBM X-Force Exchange	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
About Secunia Research | Flexera	af854a3a-2127
NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854a3a-2127
Support / Security / Advisories / / MDVSA-2013:150 | Mandriva	af854a3a-2127
Apache Tomcat - Apache Tomcat 5 vulnerabilities	af854a3a-2127
Pony Mail!	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Security Advisory SA48791 - Red Hat update for tomcat6 - Secunia	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Red Hat Customer Portal	af854a3a-2127
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	af854a3a-2127
Security Advisory SA50863 - Red Hat update for JBoss Operations Network - Secunia	af854a3a-2127
Security Advisory SA48213 - Red Hat update for jbossweb - Secunia	af854a3a-2127
Pony Mail!	af854a3a-2127
'[security bulletin] HPSBUX02741 SSRT100728 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	af854a3a-2127
Pony Mail!	af854a3a-2127
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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