CVE-2010-3718

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

Summary

CVE	CVE-2010-3718
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-10 18:00:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Apache Tomcat 7.0.0 through 7.0.3, 6.0.x, and 5.5.x, when running within a SecurityManager, does not make the ServletCo

Risk And Classification

Primary CVSS: v2.0 1.2 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

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	5.5.32	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	6.0.4	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	7.0.1	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Apache Tomcat Local bypass of security manger file permissions - SecurityReason.com	af854a3a-2127-42
Repository / Oval Repository	af854a3a-2127-42
Red Hat Customer Portal	af854a3a-2127-42

Pony Mail!	af854a3a-2127-42
Novell Sentinel Log Manager Java and Tomcat Vulnerabilities - Secunia.com	af854a3a-2127-42
mandriva.com	af854a3a-2127-42
'[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	af854a3a-2127-42
APPLE-SA-2011-10-12-3 OS X Lion v10.7.2 and Security Update 2011-006	af854a3a-2127-42
Apache Tomcat® - Apache Tomcat 7 vulnerabilities	af854a3a-2127-42
Red Hat Customer Portal	af854a3a-2127-42
Repository / Oval Repository	af854a3a-2127-42
Red Hat Customer Portal	af854a3a-2127-42
About the security content of OS X Lion v10.7.2 and Security Update 2011-006	af854a3a-2127-42
'[security bulletin] HPSBUX02725 SSRT100627 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	af854a3a-2127-42
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	af854a3a-2127-42
Apache Tomcat - Apache Tomcat 5 vulnerabilities	af854a3a-2127-42
Pony Mail!	af854a3a-2127-42
Apache Tomcat Security Manager Lets Local Users Bypass File Permissions - SecurityTracker	af854a3a-2127-42
Debian update for tomcat6 - Secunia.com	af854a3a-2127-42
Repository / Oval Repository	af854a3a-2127-42
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	af854a3a-2127-42
Red Hat Customer Portal	af854a3a-2127-42
About Secunia Research | Flexera	af854a3a-2127-42
Sentinel Log Manager 1.2.0.1 (1.2 Hot Fix 1)	af854a3a-2127-42
Debian -- Security Information -- DSA-2160-1 tomcat6	af854a3a-2127-42
'[security bulletin] HPSBUX02645 SSRT100387 rev.1 - HP-UX Apache Web Server, Remote Information Discl' - MARC	af854a3a-2127-42
'[security bulletin] HPSBST02955 rev.1 - HP XP P9000 Performance Advisor Software, 3rd party Software' - MARC	af854a3a-2127-42
IBM X-Force Exchange	af854a3a-2127-42
Pony Mail!	af854a3a-2127-42
SecurityFocus	af854a3a-2127-42
Apache Tomcat SecurityManager Security Bypass Vulnerability	af854a3a-2127-42
Pony Mail!	af854a3a-2127-42
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**