CVE-2011-5062

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

Summary

CVE	CVE-2011-5062
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-01-14 21:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x b

Risk And Classification

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

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/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	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	5.5.4	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	6.0.4	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	7.0.2	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
Debian -- Security Information -- DSA-2401-1 tomcat6	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
[security-announce] openSUSE-SU-2012:0208-1: important: tomcat6: Fix mul	af854a3a-2127-422b-91
Pony Mail!	af854a3a-2127-422b-91
[Apache-SVN] Revision 1087655	af854a3a-2127-422b-91
[Apache-SVN] Revision 1158180	af854a3a-2127-422b-91
Apache Tomcat® - Apache Tomcat 7 vulnerabilities	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
[security-announce] SUSE-SU-2012:0155-1: important: Security update for	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
[Apache-SVN] Revision 1159309	af854a3a-2127-422b-91
Apache Tomcat - Apache Tomcat 5 vulnerabilities	af854a3a-2127-422b-91
Pony Mail!	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	af854a3a-2127-422b-91
About Secunia Research | Flexera	af854a3a-2127-422b-91
'[security bulletin] HPSBST02955 rev.1 - HP XP P9000 Performance Advisor Software, 3rd party Software' - MARC	af854a3a-2127-422b-91
Pony Mail!	af854a3a-2127-422b-91
Pony Mail!	af854a3a-2127-422b-91
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.