



CVE-2014-0119

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

Summary

CVE	CVE-2014-0119
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-31 11:17:13 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that acc

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-264 | 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	6	All	All	All

Application	Apache	Tomcat	6.0	All	All	All
Application	Apache	Tomcat	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.0	alpha	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.1	alpha	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	6.0.2	alpha	All	All
Application	Apache	Tomcat	6.0.2	beta	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	6.0.35	All	All	All
Application	Apache	Tomcat	6.0.36	All	All	All
Application	Apache	Tomcat	6.0.37	All	All	All
Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.4	alpha	All	All
Application	Apache	Tomcat	6.0.5	All	All	All
Application	Apache	Tomcat	6.0.6	All	All	All

Application	Apache	Tomcat	6.0.6	alpha	All	All
Application	Apache	Tomcat	6.0.7	All	All	All
Application	Apache	Tomcat	6.0.7	alpha	All	All
Application	Apache	Tomcat	6.0.7	beta	All	All
Application	Apache	Tomcat	6.0.8	All	All	All
Application	Apache	Tomcat	6.0.8	alpha	All	All
Application	Apache	Tomcat	6.0.9	All	All	All
Application	Apache	Tomcat	6.0.9	beta	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	7.0.2	beta	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	7.0.23	All	All	All
Application	Apache	Tomcat	7.0.24	All	All	All
Application	Apache	Tomcat	7.0.25	All	All	All
Application	Apache	Tomcat	7.0.26	All	All	All
Application	Apache	Tomcat	7.0.27	All	All	All
Application	Apache	Tomcat	7.0.28	All	All	All
Application	Apache	Tomcat	7.0.29	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All
Application	Apache	Tomcat	7.0.30	All	All	All

Application	Apache	Tomcat	7.0.31	All	All	All
Application	Apache	Tomcat	7.0.32	All	All	All
Application	Apache	Tomcat	7.0.33	All	All	All
Application	Apache	Tomcat	7.0.34	All	All	All
Application	Apache	Tomcat	7.0.35	All	All	All
Application	Apache	Tomcat	7.0.36	All	All	All
Application	Apache	Tomcat	7.0.37	All	All	All
Application	Apache	Tomcat	7.0.38	All	All	All
Application	Apache	Tomcat	7.0.39	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All
Application	Apache	Tomcat	7.0.4	beta	All	All
Application	Apache	Tomcat	7.0.40	All	All	All
Application	Apache	Tomcat	7.0.41	All	All	All
Application	Apache	Tomcat	7.0.42	All	All	All
Application	Apache	Tomcat	7.0.43	All	All	All
Application	Apache	Tomcat	7.0.44	All	All	All
Application	Apache	Tomcat	7.0.45	All	All	All
Application	Apache	Tomcat	7.0.46	All	All	All
Application	Apache	Tomcat	7.0.47	All	All	All
Application	Apache	Tomcat	7.0.48	All	All	All
Application	Apache	Tomcat	7.0.49	All	All	All
Application	Apache	Tomcat	7.0.5	All	All	All
Application	Apache	Tomcat	7.0.50	All	All	All
Application	Apache	Tomcat	7.0.52	All	All	All
Application	Apache	Tomcat	7.0.53	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
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.1	All	All	All
Application	Apache	Tomcat	8.0.3	All	All	All
Application	Apache	Tomcat	8.0.5	All	All	All

City Mail
[Apache-SVN] Revision 1590028
Pony Mail!
[Apache-SVN] Revision 1589985
Support / Security / Advisories // MDVSA-2015:084 Mandriva
Pony Mail!
Red Hat Customer Portal
[Apache-SVN] Revision 1593815
Pony Mail!
[Apache-SVN] Revision 1589980
Apache Tomcat® - Apache Tomcat 6 vulnerabilities
Debian -- Security Information -- DSA-3530-1 tomcat6
[Apache-SVN] Revision 1590036
Red Hat Customer Portal
Pony Mail!
'[security bulletin] HPSBOV03503 rev.1 - HP OpenVMS CSWS_JAVA running Tomcat, Multiple Remote Vulnera' - MARC
Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
[Apache-SVN] Revision 1589983
[Apache-SVN] Revision 1588199
IBM Security Bulletin: Rational Lifecycle Adapter for HP ALM Apache Tomcat fix (CVE-2013-4286, CVE-2014-0033, CVE-2013-4322, CVE-2014-0075, CVE-2014-0095, CVE-2014-0096, CVE-2014-0097, CVE-2014-0098, CVE-2014-0099, CVE-2014-0100, CVE-2014-0101, CVE-2014-0102, CVE-2014-0103, CVE-2014-0104, CVE-2014-0105, CVE-2014-0106, CVE-2014-0107, CVE-2014-0108, CVE-2014-0109, CVE-2014-0110, CVE-2014-0111, CVE-2014-0112, CVE-2014-0113, CVE-2014-0114, CVE-2014-0115, CVE-2014-0116, CVE-2014-0117, CVE-2014-0118, CVE-2014-0119, CVE-2014-0120, CVE-2014-0121, CVE-2014-0122, CVE-2014-0123, CVE-2014-0124, CVE-2014-0125, CVE-2014-0126, CVE-2014-0127, CVE-2014-0128, CVE-2014-0129, CVE-2014-0130, CVE-2014-0131, CVE-2014-0132, CVE-2014-0133, CVE-2014-0134, CVE-2014-0135, CVE-2014-0136, CVE-2014-0137, CVE-2014-0138, CVE-2014-0139, CVE-2014-0140, CVE-2014-0141, CVE-2014-0142, CVE-2014-0143, CVE-2014-0144, CVE-2014-0145, CVE-2014-0146, CVE-2014-0147, CVE-2014-0148, CVE-2014-0149, CVE-2014-0150, CVE-2014-0151, CVE-2014-0152, CVE-2014-0153, CVE-2014-0154, CVE-2014-0155, CVE-2014-0156, CVE-2014-0157, CVE-2014-0158, CVE-2014-0159, CVE-2014-0160, CVE-2014-0161, CVE-2014-0162, CVE-2014-0163, CVE-2014-0164, CVE-2014-0165, CVE-2014-0166, CVE-2014-0167, CVE-2014-0168, CVE-2014-0169, CVE-2014-0170, CVE-2014-0171, CVE-2014-0172, CVE-2014-0173, CVE-2014-0174, CVE-2014-0175, CVE-2014-0176, CVE-2014-0177, CVE-2014-0178, CVE-2014-0179, CVE-2014-0180, CVE-2014-0181, CVE-2014-0182, CVE-2014-0183, CVE-2014-0184, CVE-2014-0185, CVE-2014-0186, CVE-2014-0187, CVE-2014-0188, CVE-2014-0189, CVE-2014-0190, CVE-2014-0191, CVE-2014-0192, CVE-2014-0193, CVE-2014-0194, CVE-2014-0195, CVE-2014-0196, CVE-2014-0197, CVE-2014-0198, CVE-2014-0199, CVE-2014-0200, CVE-2014-0201, CVE-2014-0202, CVE-2014-0203, CVE-2014-0204, CVE-2014-0205, CVE-2014-0206, CVE-2014-0207, CVE-2014-0208, CVE-2014-0209, CVE-2014-0210, CVE-2014-0211, CVE-2014-0212, CVE-2014-0213, CVE-2014-0214, CVE-2014-0215, CVE-2014-0216, CVE-2014-0217, CVE-2014-0218, CVE-2014-0219, CVE-2014-0220, CVE-2014-0221, CVE-2014-0222, CVE-2014-0223, CVE-2014-0224, CVE-2014-0225, CVE-2014-0226, CVE-2014-0227, CVE-2014-0228, CVE-2014-0229, CVE-2014-0230, CVE-2014-0231, CVE-2014-0232, CVE-2014-0233, CVE-2014-0234, CVE-2014-0235, CVE-2014-0236, CVE-2014-0237, CVE-2014-0238, CVE-2014-0239, CVE-2014-0240, CVE-2014-0241, CVE-2014-0242, CVE-2014-0243, CVE-2014-0244, CVE-2014-0245, CVE-2014-0246, CVE-2014-0247, CVE-2014-0248, CVE-2014-0249, CVE-2014-0250, CVE-2014-0251, CVE-2014-0252, CVE-2014-0253, CVE-2014-0254, CVE-2014-0255, CVE-2014-0256, CVE-2014-0257, CVE-2014-0258, CVE-2014-0259, CVE-2014-0260, CVE-2014-0261, CVE-2014-0262, CVE-2014-0263, CVE-2014-0264, CVE-2014-0265, CVE-2014-0266, CVE-2014-0267, CVE-2014-0268, CVE-2014-0269, CVE-2014-0270, CVE-2014-0271, CVE-2014-0272, CVE-2014-0273, CVE-2014-0274, CVE-2014-0275, CVE-2014-0276, CVE-2014-0277, CVE-2014-0278, CVE-2014-0279, CVE-2014-0280, CVE-2014-0281, CVE-2014-0282, CVE-2014-0283, CVE-2014-0284, CVE-2014-0285, CVE-2014-0286, CVE-2014-0287, CVE-2014-0288, CVE-2014-0289, CVE-2014-0290, CVE-2014-0291, CVE-2014-0292, CVE-2014-0293, CVE-2014-0294, CVE-2014-0295, CVE-2014-0296, CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0300, CVE-2014-0301, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0310, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0315, CVE-2014-0316, CVE-2014-0317, CVE-2014-0318, CVE-2014-0319, CVE-2014-0320, CVE-2014-0321, CVE-2014-0322, CVE-2014-0323, CVE-2014-0324, CVE-2014-0325, CVE-2014-0326, CVE-2014-0327, CVE-2014-0328, CVE-2014-0329, CVE-2014-0330, CVE-2014-0331, CVE-2014-0332, CVE-2014-0333, CVE-2014-0334, CVE-2014-0335, CVE-2014-0336, CVE-2014-0337, CVE-2014-0338, CVE-2014-0339, CVE-2014-0340, CVE-2014-0341, CVE-2014-0342, CVE-2014-0343, CVE-2014-0344, CVE-2014-0345, CVE-2014-0346, CVE-2014-0347, CVE-2014-0348, CVE-2014-0349, CVE-2014-0350, CVE-2014-0351, CVE-2014-0352, CVE-2014-0353, CVE-2014-0354, CVE-2014-0355, CVE-2014-0356, CVE-2014-0357, CVE-2014-0358, CVE-2014-0359, CVE-2014-0360, CVE-2014-0361, CVE-2014-0362, CVE-2014-0363, CVE-2014-0364, CVE-2014-0365, CVE-2014-0366, CVE-2014-0367, CVE-2014-0368, CVE-2014-0369, CVE-2014-0370, CVE-2014-0371, CVE-2014-0372, CVE-2014-0373, CVE-2014-0374, CVE-2014-0375, CVE-2014-0376, CVE-2014-0377, CVE-2014-0378, CVE-2014-0379, CVE-2014-0380, CVE-2014-0381, CVE-2014-0382, CVE-2014-0383, CVE-2014-0384, CVE-2014-0385, CVE-2014-0386, CVE-2014-0387, CVE-2014-0388, CVE-2014-0389, CVE-2014-0390, CVE-2014-0391, CVE-2014-0392, CVE-2014-0393, CVE-2014-0394, CVE-2014-0395, CVE-2014-0396, CVE-201

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)