



CVE-2013-3060

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

Summary

CVE	CVE-2013-3060
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-21 21:55:00 UTC
Updated	2016-11-28 19:09:00 UTC
Description	The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Activemq	4.0	All	All	All
Application	Apache	Activemq	4.0	m4	All	All
Application	Apache	Activemq	4.0	rc2	All	All
Application	Apache	Activemq	4.0.1	All	All	All
Application	Apache	Activemq	4.0.2	All	All	All
Application	Apache	Activemq	4.1.0	All	All	All
Application	Apache	Activemq	4.1.1	All	All	All
Application	Apache	Activemq	5.0.0	All	All	All
Application	Apache	Activemq	5.1.0	All	All	All
Application	Apache	Activemq	5.2.0	All	All	All
Application	Apache	Activemq	5.3.0	All	All	All
Application	Apache	Activemq	5.3.1	All	All	All
Application	Apache	Activemq	5.3.2	All	All	All
Application	Apache	Activemq	5.4.0	All	All	All
Application	Apache	Activemq	5.4.1	All	All	All
Application	Apache	Activemq	5.4.2	All	All	All
Application	Apache	Activemq	5.5.0	All	All	All

Application	Apache	Activemq	5.5.1	All	All	All
Application	Apache	Activemq	5.6.0	All	All	All
Application	Apache	Activemq	4.0	All	All	All
Application	Apache	Activemq	4.0	m4	All	All
Application	Apache	Activemq	4.0	rc2	All	All
Application	Apache	Activemq	4.0.1	All	All	All
Application	Apache	Activemq	4.0.2	All	All	All
Application	Apache	Activemq	4.1.0	All	All	All
Application	Apache	Activemq	4.1.1	All	All	All
Application	Apache	Activemq	5.0.0	All	All	All
Application	Apache	Activemq	5.1.0	All	All	All
Application	Apache	Activemq	5.2.0	All	All	All
Application	Apache	Activemq	5.3.0	All	All	All
Application	Apache	Activemq	5.3.1	All	All	All
Application	Apache	Activemq	5.3.2	All	All	All
Application	Apache	Activemq	5.4.0	All	All	All
Application	Apache	Activemq	5.4.1	All	All	All
Application	Apache	Activemq	5.4.2	All	All	All
Application	Apache	Activemq	5.5.0	All	All	All
Application	Apache	Activemq	5.5.1	All	All	All
Application	Apache	Activemq	5.6.0	All	All	All
Application	Apache	Activemq	All	All	All	All

References						
Reference				Source	Link	
Apache ActiveMQ CVE-2013-3060 Information Disclosure and Denial of Service Vulnerability				BID	www.securityfocus.com	
Red Hat Customer Portal				REDHAT	rhn.redhat.com	
Release Notes - ASF JIRA				CONFIRM	issues.apache.org	
fisheye6.atlassian.com/changelog/activemq				CONFIRM	fisheye6.atlassian.com	
Red Hat Customer Portal				REDHAT	rhn.redhat.com	
[AMQ-4124] Disable sample web application from out of the box broker - ASF JIRA				CONFIRM	issues.apache.org	
Apache ActiveMQ TM -- ActiveMQ 5.8.0 Release				CONFIRM	activemq.apache.org	
ActiveMQ - Dev - [DISCUSS] - ActiveMQ out of the box - Should not include the demos List View				MLIST	activemq.2283324.n4.nabb	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

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](#)