



# CVE-2014-3579

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-3579
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-10-27 19:29:00 UTC
<b>Updated</b>	2023-11-07 02:20:00 UTC
<b>Description</b>	XML external entity (XXE) vulnerability in Apache ActiveMQ Apollo 1.x before 1.7.1 allows remote consumers to have unsp

## Risk And Classification

**Problem Types:** CWE-611

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Activemq Apollo	1.0	All	All	All
Application	Apache	Activemq Apollo	1.1	All	All	All
Application	Apache	Activemq Apollo	1.2	All	All	All
Application	Apache	Activemq Apollo	1.3	All	All	All
Application	Apache	Activemq Apollo	1.4	All	All	All
Application	Apache	Activemq Apollo	1.5	All	All	All
Application	Apache	Activemq Apollo	1.6	All	All	All
Application	Apache	Activemq Apollo	1.7	All	All	All
Application	Apache	Activemq Apollo	1.0	All	All	All
Application	Apache	Activemq Apollo	1.1	All	All	All
Application	Apache	Activemq Apollo	1.2	All	All	All
Application	Apache	Activemq Apollo	1.3	All	All	All
Application	Apache	Activemq Apollo	1.4	All	All	All
Application	Apache	Activemq Apollo	1.5	All	All	All
Application	Apache	Activemq Apollo	1.6	All	All	All
Application	Apache	Activemq Apollo	1.7	All	All	All

References				
Reference	Source	Link	Tags	
[APLO-366] XPath selector - make xml parser features configurable - ASF JIRA	CONFIRM	<a href="https://issues.apache.org">issues.apache.org</a>	Issue Tr	
oss-sec: [ANNOUNCE] CVE-2014-3579 - ActiveMQ Apollo vulnerability	MLIST	<a href="https://seclists.org">seclists.org</a>	Mailing	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
<a href="https://activemq.apache.org/security-advisories.data/CVE-2014-3579-announcement.txt">activemq.apache.org/security-advisories.data/CVE-2014-3579-announcement.txt</a>	CONFIRM	<a href="https://activemq.apache.org">activemq.apache.org</a>	Vendor	
Apache ActiveMQ Apollo CVE-2014-3579 XML External Entity Injection Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Pa	
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	Issue Tr	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic	
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic	

No vendor comments have been submitted for this CVE.

Legacy QID Mappings
<a href="#">995535</a> Java (Maven) Security Update for org.apache.activemq:apollo-project (GHSA-wmhw-hpwh-44pg)

© 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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)