



# CVE-2014-3596

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

## Summary

<b>CVE</b>	CVE-2014-3596
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-08-27 00:55:00 UTC
<b>Updated</b>	2023-02-13 00:40:00 UTC
<b>Description</b>	The getCN function in Apache Axis 1.4 and earlier does not properly verify that the server hostname matches a domain nar

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Axis	1.0	All	All	All
Application	Apache	Axis	1.0	beta	All	All
Application	Apache	Axis	1.0	rc1	All	All
Application	Apache	Axis	1.0	rc2	All	All
Application	Apache	Axis	1.1	All	All	All
Application	Apache	Axis	1.1	beta	All	All
Application	Apache	Axis	1.1	rc1	All	All
Application	Apache	Axis	1.1	rc2	All	All
Application	Apache	Axis	1.2	All	All	All
Application	Apache	Axis	1.2	alpha	All	All
Application	Apache	Axis	1.2	beta1	All	All
Application	Apache	Axis	1.2	beta2	All	All
Application	Apache	Axis	1.2	beta3	All	All
Application	Apache	Axis	1.2	rc1	All	All
Application	Apache	Axis	1.2	rc2	All	All
Application	Apache	Axis	1.2	rc3	All	All
Application	Apache	Axis	1.2.1	All	All	All

Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.0	beta	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.0	rc1	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.0	rc2	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.1	beta	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.1	rc1	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.1	rc2	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	alpha	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	beta1	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	beta2	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	beta3	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	rc1	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	rc2	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2	rc3	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.2.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	1.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Axis</a>	All	All	All	All

## References

Reference	Source	Link
linux.oracle.com   ELSA-2014-1193	CONFIRM	<a href="#">linux.o</a>
IBM X-Force Exchange	XF	<a href="#">excha</a>
Pony Mail!	MLIST	<a href="#">lists.ap</a>
Security Advisory SA61222 - Oracle Linux update for axis - Secunia	SECUNIA	<a href="#">secuni</a>
Apache Axis Incomplete Fix CVE-2014-3596 SSL Certificate Validation Security Bypass Vulnerability	BID	<a href="#">www.s</a>
Pony Mail!	MISC	<a href="#">lists.ap</a>
Pony Mail!	MLIST	<a href="#">lists.ap</a>
Apache Axis Certificate Validation Flaw Lets Remote Users Spoof Server Certificates - SecurityTracker	SECTRACK	<a href="#">www.s</a>
Pony Mail!	MISC	<a href="#">lists.ap</a>
Red Hat Customer Portal	MISC	<a href="#">access</a>
[security-announce] openSUSE-SU-2019:1497-1: moderate: Security update f	SUSE	<a href="#">lists.or</a>
Red Hat Customer Portal	REDHAT	<a href="#">rhn.rec</a>

[security-announce] opensUSE-SU-2019:1526-1: moderate: Security update 1	SUSE	<a href="#">lists.ore</a>
Pony Mail!	MLIST	<a href="#">lists.ore</a>
Pony Mail!	MISC	<a href="#">lists.ore</a>
Pony Mail!	MLIST	<a href="#">lists.ore</a>
Pony Mail!	MISC	<a href="#">lists.ore</a>
[AXIS-2905] Insecure certificate validation CVE-2014-3596 - ASF JIRA	MISC	<a href="#">issues</a>
oss-security - CVE-2014-3596 - Apache Axis 1 vulnerable to MITM attack	MLIST	<a href="#">www.c</a>
Pony Mail!	MISC	<a href="#">lists.ore</a>
Oracle Critical Patch Update Advisory - January 2020	MISC	<a href="#">www.c</a>
1129935 – (CVE-2014-3596) CVE-2014-3596 axis: SSL hostname verification bypass, incomplete CVE-2012-5784 fix	MISC	<a href="#">bugzill</a>
Red Hat Customer Portal	MISC	<a href="#">access</a>
Pony Mail!	MLIST	<a href="#">lists.ore</a>
CVE-2014-3596 - Red Hat Customer Portal	MISC	<a href="#">access</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[379452](#) IBM Cognos Analytics Multiple Vulnerabilities (7123154)

[980893](#) Java (maven) Security Update for org.apache.axis:axis (GHSA-r53v-vm87-f72c)

© [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](#)