



CVE-2012-4418

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

Summary

CVE	CVE-2012-4418
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-09 23:55:00 UTC
Updated	2013-01-30 04:54:00 UTC
Description	Apache Axis2 allows remote attackers to forge messages and bypass authentication via an "XML Signature wrapping attack"

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Axis2	-	All	All	All
Application	Apache	Axis2	-	All	All	All

References

Reference	Source	Link	T
www.nds.rub.de/media/nds/veroeffentlichungen/2012/08/22/BreakingSAML_3.pdf	MISC	www.nds.rub.de	E
856755 – (CVE-2012-4418) CVE-2012-4418 axis2: vulnerable to XML signature wrapping attacks	CONFIRM	bugzilla.redhat.com	
Apache Axis2 XML Signature Wrapping Security Vulnerability	BID	www.securityfocus.com	
oss-security - CVE Request: Apache Axis2 XML Signature Wrapping Attack	MLIST	www.openwall.com	
oss-security - Re: CVE Request: Apache Axis2 XML Signature Wrapping Attack	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	ce
NVD vulnerability detail	NVD	nvd.nist.gov	ce

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[996817](#) Java (Maven) Security Update for org.apache.axis2:axis2 (GHSA-88r4-38gc-97p4)

© [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](#)