



CVE-2014-3529

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-3529
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-04 17:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The OPC SAX setup in Apache POI before 3.10.1 allows remote attackers to read arbitrary files via an OpenXML file containi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Poi	0.1	All	All	All
Application	Apache	Poi	0.10.0	All	All	All
Application	Apache	Poi	0.11.0	All	All	All
Application	Apache	Poi	0.12.0	All	All	All
Application	Apache	Poi	0.13.0	All	All	All
Application	Apache	Poi	0.14.0	All	All	All
Application	Apache	Poi	0.2	All	All	All
Application	Apache	Poi	0.3	All	All	All
Application	Apache	Poi	0.4	All	All	All
Application	Apache	Poi	0.5	All	All	All
Application	Apache	Poi	0.6	All	All	All
Application	Apache	Poi	0.7	All	All	All
Application	Apache	Poi	1.0.0	All	All	All
Application	Apache	Poi	1.0.1	All	All	All
Application	Apache	Poi	1.0.2	All	All	All
Application	Apache	Poi	1.1.0	All	All	All
Application	Apache	Poi	1.10	dev	All	All

Application	Apache	Poi	1.2.0	All	All	All
Application	Apache	Poi	1.5	All	All	All
Application	Apache	Poi	1.5.1	All	All	All
Application	Apache	Poi	1.7	dev	All	All
Application	Apache	Poi	1.8	dev	All	All
Application	Apache	Poi	2.0	All	All	All
Application	Apache	Poi	2.0	pre1	All	All
Application	Apache	Poi	2.0	pre2	All	All
Application	Apache	Poi	2.0	pre3	All	All
Application	Apache	Poi	2.0	rc1	All	All
Application	Apache	Poi	2.0	rc2	All	All
Application	Apache	Poi	2.5	All	All	All
Application	Apache	Poi	2.5.1	All	All	All
Application	Apache	Poi	3.0	All	All	All
Application	Apache	Poi	3.0	alpha1	All	All
Application	Apache	Poi	3.0	alpha2	All	All
Application	Apache	Poi	3.0	alpha3	All	All
Application	Apache	Poi	3.0.1	All	All	All
Application	Apache	Poi	3.0.2	All	All	All
Application	Apache	Poi	3.0.2	beta1	All	All
Application	Apache	Poi	3.0.2	beta2	All	All
Application	Apache	Poi	3.1	All	All	All
Application	Apache	Poi	3.1	beta1	All	All
Application	Apache	Poi	3.1	beta2	All	All
Application	Apache	Poi	3.10	beta1	All	All
Application	Apache	Poi	3.10	beta2	All	All
Application	Apache	Poi	3.2	All	All	All
Application	Apache	Poi	3.5	All	All	All
Application	Apache	Poi	3.5	beta1	All	All
Application	Apache	Poi	3.5	beta2	All	All
Application	Apache	Poi	3.5	beta3	All	All
Application	Apache	Poi	3.5	beta4	All	All
Application	Apache	Poi	3.5	beta5	All	All
Application	Apache	Poi	3.5	beta6	All	All
Application	Apache	Poi	3.6	All	All	All

Application	Apache	Poi	3.7	All	All	All
Application	Apache	Poi	3.7	beta1	All	All
Application	Apache	Poi	3.7	beta2	All	All
Application	Apache	Poi	3.7	beta3	All	All
Application	Apache	Poi	3.8	All	All	All
Application	Apache	Poi	3.8	beta1	All	All
Application	Apache	Poi	3.8	beta2	All	All
Application	Apache	Poi	3.8	beta3	All	All
Application	Apache	Poi	3.8	beta4	All	All
Application	Apache	Poi	3.8	beta5	All	All
Application	Apache	Poi	3.9	All	All	All
Application	Apache	Poi	0.1	All	All	All
Application	Apache	Poi	0.10.0	All	All	All
Application	Apache	Poi	0.11.0	All	All	All
Application	Apache	Poi	0.12.0	All	All	All
Application	Apache	Poi	0.13.0	All	All	All
Application	Apache	Poi	0.14.0	All	All	All
Application	Apache	Poi	0.2	All	All	All
Application	Apache	Poi	0.3	All	All	All
Application	Apache	Poi	0.4	All	All	All
Application	Apache	Poi	0.5	All	All	All
Application	Apache	Poi	0.6	All	All	All
Application	Apache	Poi	0.7	All	All	All
Application	Apache	Poi	1.0.0	All	All	All
Application	Apache	Poi	1.0.1	All	All	All
Application	Apache	Poi	1.0.2	All	All	All
Application	Apache	Poi	1.1.0	All	All	All
Application	Apache	Poi	1.10	dev	All	All
Application	Apache	Poi	1.2.0	All	All	All
Application	Apache	Poi	1.5	All	All	All
Application	Apache	Poi	1.5.1	All	All	All
Application	Apache	Poi	1.7	dev	All	All
Application	Apache	Poi	1.8	dev	All	All
Application	Apache	Poi	2.0	All	All	All
Application	Apache	Poi	2.0	pre1	All	All
Application	Apache	Poi	2.0	pre2	All	All

Application	Apache	Poi	2.0	pre2	All	All
Application	Apache	Poi	2.0	pre3	All	All
Application	Apache	Poi	2.0	rc1	All	All
Application	Apache	Poi	2.0	rc2	All	All
Application	Apache	Poi	2.5	All	All	All
Application	Apache	Poi	2.5.1	All	All	All
Application	Apache	Poi	3.0	All	All	All
Application	Apache	Poi	3.0	alpha1	All	All
Application	Apache	Poi	3.0	alpha2	All	All
Application	Apache	Poi	3.0	alpha3	All	All
Application	Apache	Poi	3.0.1	All	All	All
Application	Apache	Poi	3.0.2	All	All	All
Application	Apache	Poi	3.0.2	beta1	All	All
Application	Apache	Poi	3.0.2	beta2	All	All
Application	Apache	Poi	3.1	All	All	All
Application	Apache	Poi	3.1	beta1	All	All
Application	Apache	Poi	3.1	beta2	All	All
Application	Apache	Poi	3.10	beta1	All	All
Application	Apache	Poi	3.10	beta2	All	All
Application	Apache	Poi	3.2	All	All	All
Application	Apache	Poi	3.5	All	All	All
Application	Apache	Poi	3.5	beta1	All	All
Application	Apache	Poi	3.5	beta2	All	All
Application	Apache	Poi	3.5	beta3	All	All
Application	Apache	Poi	3.5	beta4	All	All
Application	Apache	Poi	3.5	beta5	All	All
Application	Apache	Poi	3.5	beta6	All	All
Application	Apache	Poi	3.6	All	All	All
Application	Apache	Poi	3.7	All	All	All
Application	Apache	Poi	3.7	beta1	All	All
Application	Apache	Poi	3.7	beta2	All	All
Application	Apache	Poi	3.7	beta3	All	All
Application	Apache	Poi	3.8	All	All	All
Application	Apache	Poi	3.8	beta1	All	All
Application	Apache	Poi	3.8	beta2	All	All
Application	Apache	Poi	3.8	beta3	All	All

Application	Apache	Poi	3.8	beta4	All	All
Application	Apache	Poi	3.8	beta5	All	All
Application	Apache	Poi	3.9	All	All	All
Application	Apache	Poi	All	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rhn.redhat.co
Red Hat Customer Portal	REDHAT	rhn.redhat.co
Apache Solr - News	CONFIRM	lucene.apach
RETIRED: POI CVE-2014-3529 Remote Security Vulnerability	BID	www.security
IBM X-Force Exchange	XF	exchange.xfo
www.apache.org/dist/poi/release/RELEASE-NOTES.txt	CONFIRM	www.apache.
Security Advisory SA59943 - Red Hat update for Red Hat JBoss BRMS - Secunia	SECUNIA	secunia.com
History of Changes	CONFIRM	poi.apache.or
Security Advisory SA61766 - Red Hat update for Red Hat JBoss Data Virtualization - Secunia	SECUNIA	secunia.com
Red Hat Customer Portal	REDHAT	rhn.redhat.co
Apache POI OpenXML parser CVE-2014-3529 XML External Entity Information Disclosure Vulnerability	BID	www.security
Red Hat Customer Portal	REDHAT	rhn.redhat.co
Security Bulletin: Vulnerabilities in Apache POI affects IBM InfoSphere Information Server	CONFIRM	www-01.ibm.c
Security Advisory SA60419 - Apache POI Two XML Entity Expansion Denial of Service Vulnerabilities - Secunia	SECUNIA	secunia.com
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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report