



CVE-2014-3004

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-3004
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-11 14:55:00 UTC
Updated	2021-10-20 11:15:00 UTC
Description	The default configuration for the Xerces SAX Parser in Castor before 1.3.3 allows context-dependent attackers to conduct >

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Castor Project	Castor	1.3	All	All	All
Application	Castor Project	Castor	1.3.1	All	All	All
Application	Castor Project	Castor	1.3	All	All	All
Application	Castor Project	Castor	1.3.1	All	All	All
Application	Castor Project	Castor	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse Project	Opensuse	12.3	All	All	All
Operating System	Opensuse Project	Opensuse	12.3	All	All	All

References

Reference	Source	Link
Cisco Bug: CSCvm56811 - Evaluation of Cisco WebEx Meetings Server Castor XML Processing	MISC	quickview.clo
Castor Library XXE Disclosure ≈ Packet Storm	MISC	packetstorms
openSUSE-SU-2014:0822-1: moderate: castor: Prevent XXE attacks	SUSE	lists.opensus
Full Disclosure: CVE-2014-3004 - Castor Library Default Config could lead to XML External Entity (XXE) Attacks	FULLDISC	seclists.org
Oracle Critical Patch Update Advisory - October 2021	MISC	www.oracle.c

Oracle Critical Patch Update Advisory - January 2020	MISC	www.oracle.c
Security Advisory SA59427 - SUSE update for castor - Secunia	SECUNIA	secunia.com
Castor Library CVE-2014-3004 XML External Entity Information Disclosure Vulnerability	BID	www.security
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](http://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