



CVE-2014-8125

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

Summary

CVE	CVE-2014-8125
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-21 17:59:00 UTC
Updated	2015-05-26 17:56:00 UTC
Description	XML external entity (XXE) vulnerability in Drools and jBPM before 6.2.0 allows remote attackers to read arbitrary files or po

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Drools	All	All	All	All
Application	Redhat	Jbpm	All	All	All	All

References

Reference	Source	Lin
BZ-1169553 - (CVE-2014-8125) EMBARGOED CVE-2014-8125 jBPM: BPMN2 file... · kiegroup/drools@c48464c · GitHub	CONFIRM	gith
Red Hat Customer Portal	REDHAT	rhn
BZ-1169553 - (CVE-2014-8125) EMBARGOED CVE-2014-8125 jBPM: BPMN2 file... · kiegroup/jbpm@713e807 · GitHub	CONFIRM	gith
Red Hat Customer Portal	REDHAT	rhn
Bug 1169553 – CVE-2014-8125 jBPM: BPMN2 file processing XXE in Process Execution	CONFIRM	bug
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

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](#) 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](#)