



CVE-2014-3630

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

Summary

CVE	CVE-2014-3630
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-29 22:29:00 UTC
Updated	2023-11-07 02:20:00 UTC
Description	XML external entity (XXE) vulnerability in the Java XML processing functionality in Play before 2.2.6 and 2.3.x before 2.3.5

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lightbend	Play Framework	2.2.0	-	All	All
Application	Lightbend	Play Framework	2.2.0	milestone1	All	All
Application	Lightbend	Play Framework	2.2.0	milestone2	All	All
Application	Lightbend	Play Framework	2.2.0	milestone3	All	All
Application	Lightbend	Play Framework	2.2.1	-	All	All
Application	Lightbend	Play Framework	2.2.2	-	All	All
Application	Lightbend	Play Framework	2.3.0	-	All	All
Application	Lightbend	Play Framework	2.3.0	rc1	All	All
Application	Lightbend	Play Framework	2.3.0	rc2	All	All
Application	Lightbend	Play Framework	2.3.1	All	All	All
Application	Lightbend	Play Framework	2.3.2	-	All	All
Application	Lightbend	Play Framework	2.3.2	rc1	All	All
Application	Lightbend	Play Framework	2.3.2	rc2	All	All
Application	Lightbend	Play Framework	2.3.3	All	All	All
Application	Lightbend	Play Framework	2.3.4	All	All	All
Application	Lightbend	Play Framework	2.2.0	-	All	All
Application	Lightbend	Play Framework	2.2.0	milestone1	All	All

Application	Lightbend	Play Framework	2.2.0	milestone2	All	All
Application	Lightbend	Play Framework	2.2.0	milestone3	All	All
Application	Lightbend	Play Framework	2.2.1	-	All	All
Application	Lightbend	Play Framework	2.2.2	-	All	All
Application	Lightbend	Play Framework	2.3.0	-	All	All
Application	Lightbend	Play Framework	2.3.0	rc1	All	All
Application	Lightbend	Play Framework	2.3.0	rc2	All	All
Application	Lightbend	Play Framework	2.3.1	All	All	All
Application	Lightbend	Play Framework	2.3.2	-	All	All
Application	Lightbend	Play Framework	2.3.2	rc1	All	All
Application	Lightbend	Play Framework	2.3.2	rc2	All	All
Application	Lightbend	Play Framework	2.3.3	All	All	All
Application	Lightbend	Play Framework	2.3.4	All	All	All
Application	Playframework	Play Framework	2.2.0	rc1	All	All
Application	Playframework	Play Framework	2.2.1	rc1	All	All
Application	Playframework	Play Framework	2.2.2	rc1	All	All
Application	Playframework	Play Framework	2.2.2	rc2	All	All
Application	Playframework	Play Framework	2.2.2	rc3	All	All
Application	Playframework	Play Framework	2.2.2	rc4	All	All
Application	Playframework	Play Framework	2.2.3	All	All	All
Application	Playframework	Play Framework	2.2.4	All	All	All
Application	Playframework	Play Framework	2.2.5	All	All	All
Application	Playframework	Play Framework	2.2.0	rc1	All	All
Application	Playframework	Play Framework	2.2.1	rc1	All	All
Application	Playframework	Play Framework	2.2.2	rc1	All	All
Application	Playframework	Play Framework	2.2.2	rc2	All	All
Application	Playframework	Play Framework	2.2.2	rc3	All	All
Application	Playframework	Play Framework	2.2.2	rc4	All	All
Application	Playframework	Play Framework	2.2.3	All	All	All
Application	Playframework	Play Framework	2.2.4	All	All	All
Application	Playframework	Play Framework	2.2.5	All	All	All

References

Reference	Source	Link	Tags
infocon.org/cons/SyScan/SyScan%202015%20Singapore/SyScan%202015%20Singapo...	MISC	infocon.org	Issue Trackin

Google Groups	CONFIRM	groups.google.com	Third Party A
Google Groups		groups.google.com	
Play Framework Security Advisory	CONFIRM	playframework.com	Issue Trackin
Google Groups		groups.google.com	
Google Groups	CONFIRM	groups.google.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

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