



CVE-2018-12533

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

Summary

CVE	CVE-2018-12533
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-18 12:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	JBoss RichFaces 3.1.0 through 3.3.4 allows unauthenticated remote attackers to inject expression language (EL) expressio

Risk And Classification

Problem Types: CWE-917

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Richfaces	All	All	All	All

References

Reference	Score
Red Hat JBoss EAP RichFaces Access Control Bug Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SE
Full Disclosure: RichFaces exploitation toolkit	FL
Red Hat Customer Portal	RE
code white Blog: Poor RichFaces	MI
Red Hat Customer Portal	RE
Malformed Request	BI
Red Hat Customer Portal	RE
CVE Program record	CV
NVD vulnerability detail	NV

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](#)