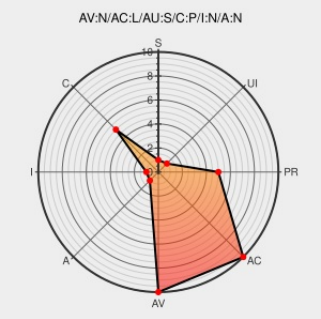
CVE-2015-3158

Published on: 08/26/2015 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:03 PM UTC

CVE-2015-3158

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Picketlink from Picketlink contain the following vulnerability:

The invokeNextValve function in identity/federation/bindings/tomcat/idp/AbstractIDPValve.java in PicketLink before 2.8.0.Beta1 does not properly check role based authorization, which allows remote authenticated users to gain access to restricted application resources via a (1) direct request or (2) request through an SP initiated flow.

CVE-2015-3158 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1669
[PLINK-708] - Checking if user is authorized right after authentication. by pedroigor · Pull Request #124 · picketlink/picketlink-bindings · GitHub	github.com text/html	CONFIRM github.com/picketlink/picketlink-bindings/pull/124
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1673
Red Hat Customer Portal	web.archive.org text/html	REDHAT RHSA-2015:1671

	Inactive Link Not Archived	
Bug 1216123 – CVE-2015-3158 PicketLink: PicketLink IDP ignores role based authorization	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1216123
[PLINK-708] Picketlink IDP does not respect role-based access constraints correctly - JBoss Issue Tracker	issues.jboss.org text/html	CONFIRM issues.jboss.org/browse/PLINK-708
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1672
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1670

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Picketlink	Picketlink	All	cr3	All	All

cpe:2.3:a:picketlink:picketlink:*:cr3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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