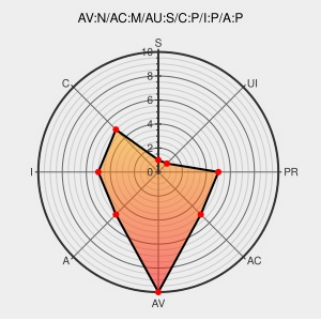
# CVE-2015-6254

Published on: 08/17/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

## CVE-2015-6254

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




Certain versions of Picketlink from Picketlink contain the following vulnerability:

The (1) Service Provider (SP) and (2) Identity Provider (IdP) in PicketLink before 2.7.0 does not ensure that the Destination attribute in a Response element in a SAML assertion matches the location from which the message was received, which allows remote attackers to have unspecified impact via unknown vectors. NOTE: this identifier was SPLIT from CVE-2015-0277 per ADT2 due to different vulnerability types.

CVE-2015-6254 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 6 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| [PLINK-680] IdP and SP must validate destination in requests and responses - JBoss Issue Tracker | issues.jboss.org, text/html | CONFIRM issues.jboss.org/browse/PLINK-680 |
| Red Hat Customer Portal | web.archive.org, text/html, Inactive Link, Not Archived | REDHAT RHSA-2015:0848 |
| Red Hat Customer Portal | web.archive.org, text/html, Inactive Link, Not Archived | REDHAT RHSA-2015:0846 |
| Bug 1194832 – CVE-2015-0277 PicketLink: SP does not take Audience condition of a SAML assertion into account | bugzilla.redhat.com, text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi? |

| | | |
|---|---|---|
| | | id=1194832 |
| Red Hat Customer Portal | web.archive.org text/html Inactive Link Not Archived | REDHAT RHSA-2015:0847 |
| Red Hat Customer Portal | web.archive.org text/html Inactive Link Not Archived | REDHAT RHSA-2015:0849 |

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 | cr5 | All | All |

cpe:2.3:a:picketlink:picketlink:*:cr5:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→