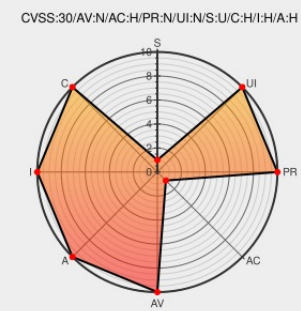
CVE-2018-14637

Published on: 11/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

CVE-2018-14637

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



Certain versions of Keycloak from Redhat contain the following vulnerability:

The SAML broker consumer endpoint in Keycloak before version 4.6.0.Final ignores expiration conditions on SAML assertions. An attacker can exploit this vulnerability to perform a replay attack.

CVE-2018-14637 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **keycloak** version **4.6.0.Final**

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
1627851 – (CVE-2018-14637) CVE-2018-14637 keycloak: expiration not validated in SAML broker consumer endpoint	Issue Tracking Third Party Advisory bugzilla.redhat.com	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14637

text/html

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.

Related QID Numbers

981087 Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-gf2j-7qwg-4f5x)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→