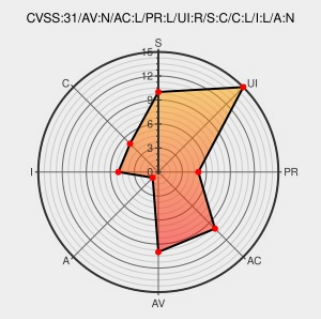
CVE-2020-1697

Published on: 02/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:46 PM UTC

CVE-2020-1697

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



Certain versions of Keycloak from Redhat contain the following vulnerability:

It was found in all keycloak versions before 9.0.0 that links to external applications (Application Links) in the admin console are not validated properly and could allow Stored XSS attacks. An authed malicious user could create URLs to trick users in other realms, and possibly conduct further attacks.

CVE-2020-1697 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **keycloak** version **All versions before 9.0.0**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
1791538 – (CVE-2020-1697) CVE-2020-1697 keycloak: stored XSS in	Issue Tracking	CONFIRM

client settings via application links

Third Party Advisory
bugzilla.redhat.com
text/html

bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1697

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	Redhat	Keycloak	All	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Single Sign-on	7.3	All	All	All
Application	Redhat	Single Sign-on	7.3	All	All	All

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

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

cpe:2.3:a:redhat:single_sign-on:7.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:single_sign-on:7.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→