



CVE-2020-10776

Published on: 11/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:33 PM UTC

CVE-2020-10776

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Keycloak](#) from [Redhat](#) contain the following vulnerability:

A flaw was found in Keycloak before version 12.0.0, where it is possible to add unsafe schemes for the redirect_uri parameter. This flaw allows an attacker to perform a Cross-site scripting attack.

CVE-2020-10776 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
1847428 – (CVE-2020-10776) CVE-2020-10776 keycloak: OIDC redirect_uri allows dangerous schemes resulting in potential XSS	Issue Tracking Mitigation Vendor Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1847428

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
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→