



CVE-2020-10686

Published on: 05/04/2020 12:00:00 AM UTC

Last Modified on: 08/05/2022 07:32:00 PM UTC

CVE-2020-10686

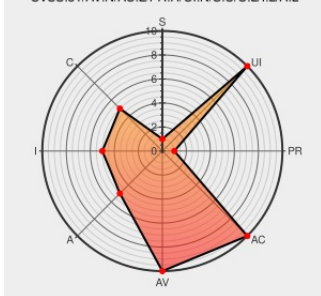
Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L



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

A flaw was found in Keycloak version 8.0.2 and 9.0.0, and was fixed in Keycloak version 9.0.1, where a malicious user registers as oneself. The attacker could then use the remove devices form to post different credential IDs and possibly remove MFA devices for other users.

CVE-2020-10686 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Keycloak** - **keycloak** version **8.0.2**

Affected Vendor/Software: **Keycloak** - **keycloak** version **9.0.0**

CVSS3 Score: **4.7 - MEDIUM**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2020-10686 (CVE-2020-10686) CVE-2020-10686	CVE-2020-10686	CONFIRM

1814609 – (CVE-2020-10686) CVE-2020-10686 keycloak: remove other users MFA devices

Issue Tracking

Vendor Advisory

bugzilla.redhat.com

text/html

CONFIRM

bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10686

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	8.0.2	All	All	All
Application	Redhat	Keycloak	9.0.0	All	All	All
Application	Redhat	Keycloak	8.0.2	All	All	All
Application	Redhat	Keycloak	9.0.0	All	All	All

cpe:2.3:a:redhat:keycloak:8.0.2:*****:

cpe:2.3:a:redhat:keycloak:9.0.0:*****:

cpe:2.3:a:redhat:keycloak:8.0.2:*****:

cpe:2.3:a:redhat:keycloak:9.0.0:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @LinInfoSec	Keycloak - CVE-2020-10686: bugzilla.redhat.com/show_bug.cgi?i...	2022-08-05 21:01:42
 @RemotelyAlerts	Severity: ?? A flaw was found in Keycloak version 8.0... CVE-2020-10686 Link for more: alerts.remotelyrmm.com/CVE-2020-10686	2022-08-05 21:31:46

← Previous ID

Next ID →