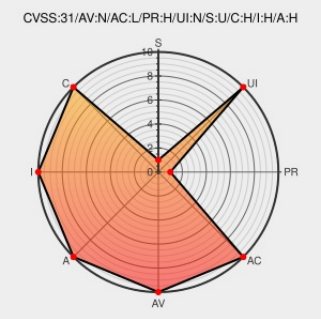
CVE-2019-10169

Published on: 05/08/2020 12:00:00 AM UTC

Last Modified on: 10/19/2021 01:54:00 PM UTC

CVE-2019-10169

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



Certain versions of Keycloak from Redhat contain the following vulnerability:

A flaw was found in Keycloak's user-managed access interface, where it would permit a script to be set in the UMA policy. This flaw allows an authenticated attacker with UMA permissions to configure a malicious script to trigger and execute arbitrary code with the permissions of the user running application.

CVE-2019-10169 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **keycloak** version **8.0.0**

CVSS3 Score: 7.2 - HIGH

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

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
1721302 – (CVE-2019-10169) CVE-2019-10169 keycloak: script	Issue Tracking	CONFIRM

execution via UMA policy trigger

Vendor Advisory
bugzilla.redhat.com
text/html

bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10169

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→