



CVE-2020-1744

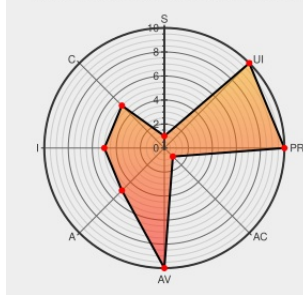
Published on: 03/24/2020 12:00:00 AM UTC

Last Modified on: 11/16/2022 03:13:00 AM UTC

CVE-2020-1744

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/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 before version 9.0.1. When configuring an Conditional OTP Authentication Flow as a post login flow of an IDP, the failure login events for OTP are not being sent to the brute force protection event queue. So BruteForceProtector does not handle this events.

CVE-2020-1744 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Red Hat** - **keycloak** version **all keycloak versions prior to 9.0.1**

CVSS3 Score: **5.6 - MEDIUM**

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

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
1805792 – (CVE-2020-1744) CVE-2020-1744 keycloak: failedLogin Event not	Issue Tracking	CONFIRM

sent to BruteForceProtector when using Post Login Flow with Conditional-OTP

Vendor Advisory

bugzilla.redhat.com

text/html

bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1744

Red Hat Customer Portal

Vendor Advisory

access.redhat.com

text/html

 CONFIRM

access.redhat.com/security/cve/CVE-2020-1744

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

980852 Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-4gf2-xv97-63m2)

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)
 @LinInfoSec	Keycloak - CVE-2020-1744: access.redhat.com/security/cve/C...	2022-11-16 07:01:20

← Previous ID

Next ID →