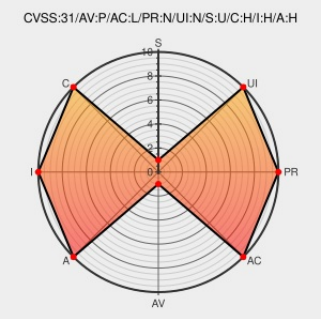
CVE-2021-20262

Published on: 03/09/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 10:10:56 PM UTC

CVE-2021-20262

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



Certain versions of Keycloak from Redhat contain the following vulnerability:

A flaw was found in Keycloak 12.0.0 where re-authentication does not occur while updating the password. This flaw allows an attacker to take over an account if they can obtain temporary, physical access to a user's browser. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.

CVE-2021-20262 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.8 - MEDIUM

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
1933639 – (CVE-2021-20262) CVE-2021-20262 keycloak: missing re-authentication while updating password	Issue Tracking Vendor Advisory bugzilla.redhat.com	MISC bugzilla.redhat.com/show_bug.cgi?id=1933639

text/html

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

982882 Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-xf46-8vvp-4hxx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Keycloak	12.0.0	All	All	All
Application	Redhat	Keycloak	12.0.0	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All

cpe:2.3:a:redhat:keycloak:12.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:keycloak:12.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:single_sign-on:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:single_sign-on:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→