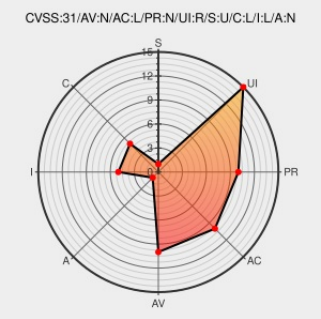
CVE-2020-1728

Published on: 04/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:46 PM UTC

CVE-2020-1728

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



Certain versions of Quarkus from Quarkus contain the following vulnerability:

A vulnerability was found in all versions of Keycloak where, the pages on the Admin Console area of the application are completely missing general HTTP security headers in HTTP-responses. This does not directly lead to a security issue, yet it might aid attackers in their efforts to exploit other problems. The flaws unnecessarily make the servers more prone to Clickjacking, channel downgrade attacks and other similar client-based attack vectors.

CVE-2020-1728 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
1800585 – (CVE-2020-1728) CVE-2020-1728 keycloak: security headers missing on REST endpoints	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1728

Related QID Numbers

982984 Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-3gg7-9q2x-79fc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quarkus	Quarkus	All	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Keycloak	All	All	All	All

cpe:2.3:a:quarkus:quarkus:*:*:*:*:*:*:*:*:

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→