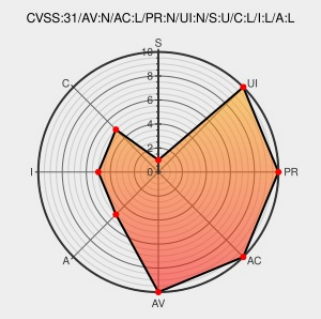
CVE-2020-14359

Published on: 02/23/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:53 PM UTC

CVE-2020-14359

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



Certain versions of Keycloak from Redhat contain the following vulnerability:

A vulnerability was found in all versions of Keycloak Gatekeeper, where on using lower case HTTP headers (via cURL) an attacker can bypass our Gatekeeper. Lower case headers are also accepted by some webservers (e.g. Jetty). This means there is no protection when we put a Gatekeeper in front of a Jetty server and use lowercase headers.

CVE-2020-14359 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Login server redirect	Issue Tracking Third Party Advisory	MISC issues.jboss.org/browse/KEYCLOAK-

	issues.jboss.org text/html	14090
1868591 – (CVE-2020-14359) CVE-2020-14359 keycloak: gatekeeper bypass via cURL when using lower case HTTP headers	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1868591

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	All	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Louketo Proxy	All	All	All	All

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

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

cpe:2.3:a:redhat:louketo_proxy:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→