



CVE-2020-10758

Published on: 09/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:33 PM UTC

CVE-2020-10758

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

Certain versions of [Keycloak](#) from [Redhat](#) contain the following vulnerability:

A vulnerability was found in Keycloak before 11.0.1 where DoS attack is possible by sending twenty requests simultaneously to the specified keycloak server, all with a Content-Length header value that exceeds the actual byte count of the request body.

CVE-2020-10758 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
1843849 – (CVE-2020-10758) CVE-2020-10758 keycloak: DoS by sending multiple simultaneous requests with a Content-	Issue Tracking Mitigation Vendor Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1843849

Length header value greater than actual byte count of request body

KEYCLOAK-14872 CL DoS · keycloak/keycloak@bee4ca8 · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC
github.com/keycloak/keycloak/commit/bee4ca89897766c4b68856eafe14f1a3dad34251

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	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Openshift Application Runtimes	1.0	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Openshift Application Runtimes	1.0	All	All	All
Application	Redhat	Single Sign-on	-	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Single Sign-on	7.4	All	All	All
Application	Redhat	Single Sign-on	-	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Single Sign-on	7.4	All	All	All

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

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

cpe:2.3:a:redhat:openshift_application_runtimes:-:***:text-only:***:

cpe:2.3:a:redhat:openshift_application_runtimes:1.0:*****:

cpe:2.3:a:redhat:openshift_application_runtimes:-:***:text-only:***:

cpe:2.3:a:redhat:openshift_application_runtimes:1.0:*****:

cpe:2.3:a:redhat:single_sign-on:-:***:text-only:***:

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

cpe:2.3:a:redhat:single_sign-on:7.4:*****:

cpe:2.3:a:redhat:single_sign-on:7.4:*:*:*:*:
cpe:2.3:a:redhat:single_sign-on:-:*:*:text-only:*:*:
cpe:2.3:a:redhat:single_sign-on:7.0:*:*:*:*:*:
cpe:2.3:a:redhat:single_sign-on:7.4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Posted (UTC)

Next ID→

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report