



CVE-2017-12160

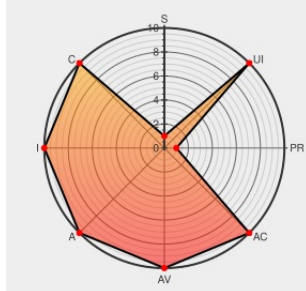
Published on: 10/26/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

CVE-2017-12160

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

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



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

It was found that Keycloak oauth would permit an authenticated resource to obtain an access/refresh token pair from the authentication server, permitting indefinite usage in the case of permission revocation. An attacker on an already compromised resource could use this flaw to grant himself continued permissions and possibly conduct further

attacks.

CVE-2017-12160 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Red Hat, Inc.** - **keycloak** version **3.4.0**

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Red Hat Customer Portal	Issue Tracking Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2017:2906
1484154 – (CVE-2017-12160) CVE-2017-12160 keycloak: resource privilege extension via access token in oauth	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1484154
Red Hat Customer Portal	Issue Tracking Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2017:2904
Red Hat Customer Portal	Issue Tracking Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2017:2905
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
Application	Redhat	Keycloak	-	All	All	All
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 →
-------------------------------	---------------------------