



CVE-2016-8609

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-8609
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-01 17:29:00 UTC
Updated	2023-11-07 02:36:00 UTC
Description	It was found that the keycloak before 2.3.0 did not implement authentication flow correctly. An attacker could use this flaw to

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
RedHat keycloak CVE-2016-8609 Session Hijacking Vulnerability	BID
Red Hat Customer Portal	REDHA
Red Hat Single Sign-On Keycloak Authentication Flow Error Lets Remote Users Hijack the Target User's Session - SecurityTracker	SECTR
1386729 – (CVE-2016-8609) CVE-2016-8609 keycloak: account hijacking via auth code fixation	CONFIL
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981171](#) Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-95m6-mjh3-58gm)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)