

Keycloak-quarkus-server: keycloak path trasversal

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-10492
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-25 08:15:08 UTC
Updated	2026-05-06 19:16:34 UTC
Description	A vulnerability was found in Keycloak. A user with high privileges could read sensitive information from a Vault file that is nc

Risk And Classification

Primary CVSS: v3.0 2.7 LOW from secalert@redhat.com

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

Problem Types: CWE-73 | CWE-73 External Control of File Name or Path

Version	Source	Type	Score	Severity	Vector
3.0	secalert@redhat.com	Secondary	2.7	LOW	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
3.0	CNA	CVSS	2.7	LOW	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak 24	unaffected 24.0.9-1 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 24	unaffected 24-18 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 24	unaffected 24-18 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 24.0.9	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0.6-2 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-5 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-6 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0.6	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified	Not specified

References			
Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2024-10492	secalert@redhat.com	access.redhat.com	
github.com/keycloak/keycloak/pull/35223	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2024:10178	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2024:10175	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
github.com/keycloak/keycloak/issues/35215	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2024:10176	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2024:10177	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit	
Discovery Credit	
CNA: Red Hat would like to thank Brahim Raddahi (is4u.be) for reporting this issue. (en)	

Additional Advisory Data		
Source	Time	Event

Source	Time	Event
CNA	2024-10-29T00:00:00.000Z	Reported to Red Hat.
CNA	2024-11-21T16:56:00.000Z	Made public.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)