



Bug 2322447 (CVE-2024-10492) - CVE-2024-10492 keycloak-quarkus-server: Keycloak path trasversal

Keywords: Security ✕

Reported: 2024-10-29 13:16 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-04-30 04:01 UTC ([History](#))

Alias: CVE-2024-10492

CC List: 31 users ([show](#))

Deadline: 2024-11-21

Fixed In Version:

Product: Security Response

Clone Of:

Component: vulnerability

Environment:

Last Closed:

Embargoed:

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:


TreeView+ [depends on](#) / [blocked](#)

Attachments [\(Terms of Use\)](#)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:10175	0	None	None	None	2024-11-21 19:23:28 UTC
Red Hat Product Errata	RHSA-2024:10176	0	None	None	None	2024-11-21 19:24:01 UTC
Red Hat	RHSA-2024:10177	0	None	None	None	2024-11-21

Product Errata						19:24:32 UTC
Red Hat Product Errata	RHSA-2024:10178	0	None	None	None	2024-11-21 19:24:58 UTC

OSIDB Bzimport  2024-10-29 13:16:46 UTC[Description](#)

A vulnerability was found in Keycloak. A user with high privileges could read sensitive information from a Vault file that is not within the expected context.

In Keycloak 24.0.8, a vulnerability allows unauthorized file access through path traversal in file vault configurations due to permissive regex validation. This weakness allows reading any file to the Keycloak server, but the admin user will not be able to access the contents unless they have also compromised the remote system that the password/secret is intended to be sent to. In practical terms, the only information leaked to the admin user is the existence of the file.

Version affected: <= 26.0.2

errata-xmlrpc 2024-11-21 19:23:26 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 24

Via [RHSA-2024:10175](#) <https://access.redhat.com/errata/RHSA-2024:10175>

errata-xmlrpc 2024-11-21 19:23:59 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 24.0.9

Via [RHSA-2024:10176](#) <https://access.redhat.com/errata/RHSA-2024:10176>

errata-xmlrpc 2024-11-21 19:24:29 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 26.0

Via RHSA-2024:10177 <https://access.redhat.com/errata/RHSA-2024:10177>

errata-xmlrpc 2024-11-21 19:24:55 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 26.0.6

Via RHSA-2024:10178 <https://access.redhat.com/errata/RHSA-2024:10178>

Chess Hazlett 2024-11-27 20:35:18 UTC

[Comment 5](#)

upstream commit:

<https://github.com/keycloak/keycloak/pull/35223/commits/9fe3c398560575b8c51e41f5ba7823b760978472>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

