CVE-2025-1391

VEX

Public on February 17, 2025
Last modified: May 6, 2026 at 4:48:36 PM UTC

MODERATE

Moderate severity
What does this mean?

5.4

CVSS v3 Score Breakdown

Jump to section

Description | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | FAQ

Description

A flaw was found in the Keycloak organization feature, which allows the incorrect assignment of an organization to a user if their username or email matches the organization’s domain pattern. This issue occurs at the mapper level, leading to misrepresentation in tokens. If an application relies on these claims for authorization, it may incorrectly assume a user belongs to an organization they are not a member of, potentially granting unauthorized access or privileges.

Additional information

- Bugzilla 2346082: keycloak-services: Improper Authorization in Keycloak Organization Mapper Allows Unauthorized Organization Claims
- CWE-284: Improper Access Control

External references

- https://www.cve.org/CVERecord?id=CVE-2025-1391
- https://nvd.nist.gov/vuln/detail/CVE-2025-1391
- https://github.com/keycloak/keycloak/issues/37169
- https://github.com/keycloak/keycloak/pull/37235

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Build of Keycloak
Components	keycloak-services
State	Fixed
Justification	None
Errata	RHSA-2025:2545
Release Date	March 10, 2025

Products / Services	Red Hat build of Keycloak 26.0
Components	rhbk/keycloak-operator-bundle
State	Fixed
Justification	None
Errata	RHSA-2025:2544
Release Date	March 10, 2025

Products / Services	Red Hat build of Keycloak 26.0
Components	rhbk/keycloak-rhel9
State	Fixed
Justification	None
Errata	RHSA-2025:2544

1 of 1

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	5.4	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	Low	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	Low	N/A	N/A
Integrity Impact	Low	N/A	N/A
Availability Impact	None	N/A	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

Understanding the Weakness (CWE)

CWE-284

Other

Technical Impact:Varies by Context

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors?
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?
- What can I do if my product is listed as "Will not fix"?
- What can I do if my product is listed as "Fix deferred"?
- What is a mitigation?
- I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: May 6, 2026 at 4:48:36 PM UTC