Bug 2346082 (CVE-2025-1391) - CVE-2025-1391 keycloak-services: Improper Authorization in Keycloak Organization Mapper Allows Unauthorized Organization Claims

Keywords: Security

Status: NEW

Alias: CVE-2025-1391

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2025-02-17 08:58 UTC by OSIDB Bzimport

Modified: 2025-03-10 18:17 UTC (History)

CC List: 11 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2025:2544	0	None	None	None	2025-03-10 18:17:46 UTC
Red Hat Product Errata	RHSA-2025:2545	0	None	None	None	2025-03-10 18:02:59 UTC

OSIDB Bzimport 2025-02-17 08:58:22 UTC Description

This vulnerability is caused by the improper mapping of users to organizations based solely on email/username patterns. The issue is limited to the token claim level, meaning the user is not truly added to the organization but may appear as such in applications relying on these claims. The risk increases in scenarios where self-registration is enabled and unrestricted, allowing an attacker to exploit the naming pattern. The issue is mitigated if admins restrict registration or use strict validation mechanisms.

errata-xmlrpc 2025-03-10 18:02:58 UTC Comment 1

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2025:2545 https://access.redhat.com/errata/RHSA-2025:2545

errata-xmlrpc 2025-03-10 18:17:44 UTC Comment 2

This issue has been addressed in the following products:

Red Hat build of Keycloak 26.0

Via RHSA-2025:2544 https://access.redhat.com/errata/RHSA-2025:2544

Note

You need to log in before you can comment on or make changes to this bug.