Bug 2439081 (CVE-2026-2366) - CVE-2026-2366 keycloak: Keycloak: Information disclosure via authorization bypass in Admin API

Keywords: Security ×

Status: NEW

Alias: CVE-2026-2366

Product: Security Response

Component: vulnerability

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

Reported: 2026-02-11 19:58 UTC by OSIDB Bzimport

Modified: 2026-02-11 20:08 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-02-11 19:58:19 UTC Description

```
Summary

An authorization bypass exists in the Keycloak Admin API where
the endpoint /admin/realms/

{realm}/organizations/members/{member-id}/organizations fails
to perform necessary permission checks. This allows any
authenticated user, regardless of their roles or
administrative privileges, to enumerate the organization
memberships of any other user if their unique identifier
(UUID) is known.

Requirements to exploit
* The Organizations feature must be enabled (which is the
```

default in recent versions).
* The attacker must possess a valid access token for the realm.
* The attacker must know the UUID of the victim user.
Component affected

org.keycloak.services.resources.admin.organizations

Version affected: 26.5.1

Patch available: No

CVSS: 3.1 (Low) CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

Embargo: No

Acknowledgement: Reynaldo Immanuel, Joy Gilbert

Steps to reproduce
Enable the Organizations feature and create multiple organizations (e.g., orgA, orgB).
Create a victim user and assign them to several organizations
Create a low-privileged "attacker" user with no administrative roles.
Obtain an OIDC access token for the low-privileged user.
Execute a GET request to /admin/realms/{realm}/organizations/members/

{victim-id}
/organizations using the low-privileged token.

Observe that the server returns a 200 OK response containing a full list of the victim's organization memberships instead of the expected 403 Forbidden.

Note

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