



Bug 2442277 (CVE-2026-3121) - CVE-2026-3121 keycloak: org.keycloak/keycloak-services: Keycloak: Privilege escalation via manage-clients permission

Keywords: ✕ ▼

Reported: 2026-02-24 13:09 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-24 13:39 UTC ([History](#))

Alias: CVE-2026-3121

CC List: 27 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

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](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-24 13:09:20 UTC

[Description](#)

An admin with manage-clients permission, has always access to manage permissions via the permissions client and, therefore, can escalate privileges to assign to him or other admins permissions to manage roles, users or whatever. Right now `manage-clients` is exactly the same than manage-permissions. Requirements to exploit: The attacker should be a `manage-clients` administrator in keycloak and the realm should be configure with admin permissions (enabled at realm level). Reproducer
In a keycloak realm enable admin permissions in Realm Settings -> General.

Create an admin user and grant to him manage, view and list

clients.

Note

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

