Bug 2422596 (CVE-2025-14777) - CVE-2025-14777 keycloak: Keycloak IDOR in realm client creating/deleting

Keywords: Security

Status: NEW

Alias: CVE-2025-14777

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: 2025-12-16 04:58 UTC by OSIDB Bzimport

Modified: 2025-12-16 05:00 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-12-16 04:58:37 UTC Description

An IDOR (Broken Access Control) vulnerability exists in the admin API endpoints for authorization resource management, specifically in ResourceSetService and PermissionTicketService. The system checks authorization against the resourceServer (client) ID provided in the API request, but the backend database lookup and modification operations (findById, delete) only use the resourceId. This mismatch allows an authenticated attacker with fine-grained admin permissions for one client (e.g., Client A) to delete or update resources belonging to another client (Client B) within the same realm by supplying a valid resource ID.

Note

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