Bug 2419086 (CVE-2025-14083) - CVE-2025-14083 keycloak-server: Keycloak: Improper Access Control in Admin REST API leads to information disclosure

Keywords: Security

Status: NEW

Alias: CVE-2025-14083

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: 2025-12-05 06:11 UTC by OSIDB Bzimport

Modified: 2026-01-21 11:26 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-12-05 06:11:16 UTC Description

An Improper Access Control vulnerability exists in the Keycloak Admin REST API, where a user possessing only the create-client permission—considered low-privilege by design—can unexpectedly access the /admin/realms/master/users/profile endpoint. This endpoint returns internal user profile schema data, including attribute names, validation rules, display metadata, and permission mappings. Although the attacker cannot view actual user accounts, the exposure of backend schema and rules results from insufficient authorization checks specifically on this endpoint. An authenticated but minimally privileged user can remotely retrieve sensitive configuration metadata, which may be leveraged to craft targeted attacks or prepare future privilege-escalation

attempts.

Note

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