Bug 2419078 (CVE-2025-14082) - CVE-2025-14082 keycloak-services: Keycloak Admin REST API: Improper Access Control leads to sensitive role metadata information disclosure

Keywords: Security

Status: NEW

Alias: CVE-2025-14082

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 05:31 UTC by OSIDB Bzimport

Modified: 2025-12-10 08:37 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 05:31:45 UTC Description

```
Improper Access Control vulnerability in the Keycloak Admin
REST API. A user possessing only the built-in role_query-
groups permission can retrieve the complete list of realm
roles, including sensitive administrator-created roles and
internal metadata. Although the user cannot access full role
details or modify configurations, this unintended exposure of
role names, IDs, composite status, and container identifiers
stems from insufficient authorization checks on the
/admin/realms/{realm}/roles endpoint. A remote authenticated
attacker with high-privileged (but restricted) access can
leverage this information disclosure to map privilege
structures and plan targeted privilege-escalation attempts,
```

affecting the confidentiality of Keycloak deployments.

Note

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