Bug 2442572 (CVE-2026-3190) - CVE-2026-3190 keycloak: Keycloak: Information Disclosure via improper role enforcement in UMA 2.0 Protection API

Keywords: Security

Status: NEW

Alias: CVE-2026-3190

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: 2026-02-25 08:34 UTC by OSIDB Bzimport

Modified: 2026-02-27 10:06 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-02-25 08:34:37 UTC Description

```
Summary

The UMA 2.0 Protection API endpoint for permission tickets
fails to enforce the uma_protection role check. This allows
any authenticated user with a token issued for a resource
server client to enumerate all permission tickets in the
system.

Requirements to exploit:

An attacker must possess a valid, authenticated user token for
```

a resource server client that lacks the uma_protection role.

Note

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