Bug 2455324 (CVE-2026-37977) - CVE-2026-37977 keycloak: org.keycloak.protocol.oidc.grants.ciba: Keycloak: Information disclosure via CORS header injection due to unvalidated JWT azp claim

Keywords: Security ×

Status: NEW

Alias: CVE-2026-37977

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: 2026-04-06 07:50 UTC by OSIDB Bzimport

Modified: 2026-04-06 08:34 UTC (History)

CC List: 9 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-06 07:50:01 UTC Description

```
CORS header injection vulnerability in Keycloak’s UMA token
endpoint. The flaw is caused by reading the azp claim from a
client-supplied JWT to set the Access-Control-Allow-Origin
header before the JWT signature is validated. When a specially
crafted JWT with an attacker-controlled azp value is
processed, that value is reflected as the CORS origin even
though the grant is later rejected. This can be exploited
remotely without authentication when a target client is
misconfigured with webOrigins: ["*"]. Attackers can then read
UMA error responses cross-origin, weakening origin isolation
and exposing low-sensitivity information from the
```

```
authorization server.
```

Note

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