Bug 2430314 (CVE-2026-1035) - CVE-2026-1035 org.keycloak.protocol.oidc: Keycloak Refresh Token Reuse Bypass via TOCTOU Race Condition

Keywords: Security

Status: NEW

Alias: CVE-2026-1035

Deadline: 2026-01-16

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: 2026-01-16 07:15 UTC by OSIDB Bzimport

Modified: 2026-02-18 08:28 UTC (History)

CC List: 27 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-01-16 07:15:01 UTC Description

A race condition (Time-of-Check to Time-of-Use) exists in the TokenManager class, specifically within the validateTokenReuse method. This vulnerability allows an attacker to bypass the refreshTokenMaxReuse security policy when it is set to zero (strict single-use). By sending concurrent requests, a single refresh token can be exchanged for multiple valid access tokens before the usage counter is updated, undermining the Refresh Token Rotation hardening measure.

Note

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