



Bug 2448351 (CVE-2026-4325) - CVE-2026-4325 keycloak: Keycloak: Replay of action tokens via improper handling of single-use entries

Keywords: Security

Reported: 2026-03-17 12:46 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-04-02 12:35 UTC ([History](#))

Alias: CVE-2026-4325

CC List: 9 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-03-17 12:46:42 UTC

[Description](#)

Keycloak's SingleUseObjectProvider is a global flat key-value store used without type or namespace isolation. This allows an attacker to delete arbitrary single-use entries, enabling the replay of consumed action tokens such as password reset links. Requirements to exploit:

Note

You need to [log in](#) before you can comment on or make changes to this bug.

