Bug 2353868 (CVE-2025-2559) - CVE-2025-2559 org.keycloak/keycloak-services: JWT Token Cache Exhaustion Leading to Denial of Service (DoS) in Keycloak

Keywords: Security

Status: NEW

Alias: CVE-2025-2559

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: 2025-03-20 12:25 UTC by OSIDB Bzimport

Modified: 2026-04-30 04:01 UTC (History)

CC List: 34 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2025:4335	0	None	None	None	2025-04-29 23:03:23 UTC
Red Hat Product Errata	RHSA-2025:4336	0	None	None	None	2025-04-29 22:53:32 UTC

OSIDB Bzimport 2025-03-20 12:25:01 UTC Description

A trusted client with long-lived JWT tokens can cause memory exhaustion in Keycloak due to unbounded token caching.

errata-xmlrpc 2025-04-29 22:53:29 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat build of Keycloak 22

Via RHSA-2025:4336 https://access.redhat.com/errata/RHSA-2025:4336

errata-xmlrpc 2025-04-29 23:03:19 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat build of Keycloak 26.0

Via RHSA-2025:4335 https://access.redhat.com/errata/RHSA-2025:4335

Note

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