Org.keycloak/keycloak-services: jwt token cache exhaustion leading to denial of service (dos) in keycloak

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-2559
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-25 09:15:17 UTC
Updated	2026-05-06 17:16:19 UTC
Description	A flaw was found in Keycloak. When the configuration uses JWT tokens for authentication, the tokens are cached until expi

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-770 | CWE-770 Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

vailability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0.11-2 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-12 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-13 * rpm	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
github.com/keycloak/keycloak/issues/38576	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2025:4335	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:4336	secalert@redhat.com	access.redhat.com	
github.com/keycloak/keycloak/commit/a10c8119d4452b866b90a9019b2cc1599192...	secalert@redhat.com	github.com	
access.redhat.com/security/cve/CVE-2025-2559	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-03-20T11:46:08.046Z	Reported to Red Hat.
CNA	2025-03-20T00:00:00.000Z	Made public.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report