Keycloak: keycloak tls client-initiated renegotiation denial of service

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

Summary

CVE	CVE-2025-11419
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-23 21:15:46 UTC
Updated	2026-04-20 18:16:22 UTC
Description	A flaw was found in Keycloak. This vulnerability allows an unauthenticated remote attacker to cause a denial of service (Do

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

EPSS: 0.000460000 probability, percentile 0.142470000 (date 2026-04-21)

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	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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 26.0	unaffected 26.0.16-2 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-20 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-21 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0.16	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2.10-2 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-11 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-11 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2.10	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2025-11419	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2025:18890	secalert@redhat.com	access.redhat.com	
github.com/keycloak/keycloak/issues/43020	secalert@redhat.com	github.com	
github.com/keycloak/keycloak/discussions/25209	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2025:18254	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:18889	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:18255	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-10-07T11:12:36.431Z	Reported to Red Hat.
CNA	2025-10-07T00:00:00.000Z	Made public.

Workarounds

CNA: To mitigate this vulnerability, configure Keycloak to reject client-initiated TLS renegotiation by adding the following Java system property to the Keycloak startup configuration: -Djdk.tls.rejectClientInitiatedRenegotiation=true This prevents unauthenticated attackers from triggering repeated TLS renegotiations and exhausting server CPU resources. Additionally, ensure that Keycloak is deployed behind proper network access controls and rate-limiting mechanisms to further reduce exposure to DoS attacks.

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