



# Keycloak: keycloak tls client-initiated renegotiation denial of service

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2025-11419  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | redhat  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2025-12-23 21:15:46 UTC   |
| <b>Updated</b>         | 2026-04-20 18:16:22 UTC   |
| <b>Description</b>     | 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

Integrity

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                |
|---|---------------------|---|---------------------|
| <a href="https://access.redhat.com/security/cve/CVE-2025-11419">access.redhat.com/security/cve/CVE-2025-11419</a>   | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     |                     |
| <a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>                             | secalert@redhat.com | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a> |                     |
| <a href="https://access.redhat.com/errata/RHSA-2025:18890">access.redhat.com/errata/RHSA-2025:18890</a>             | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     |                     |
| <a href="https://github.com/keycloak/keycloak/issues/43020">github.com/keycloak/keycloak/issues/43020</a>           | secalert@redhat.com | <a href="https://github.com">github.com</a>                   |                     |
| <a href="https://github.com/keycloak/keycloak/discussions/25209">github.com/keycloak/keycloak/discussions/25209</a> | secalert@redhat.com | <a href="https://github.com">github.com</a>                   |                     |
| <a href="https://access.redhat.com/errata/RHSA-2025:18254">access.redhat.com/errata/RHSA-2025:18254</a>             | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     |                     |
| <a href="https://access.redhat.com/errata/RHSA-2025:18889">access.redhat.com/errata/RHSA-2025:18889</a>             | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     |                     |
| <a href="https://access.redhat.com/errata/RHSA-2025:18255">access.redhat.com/errata/RHSA-2025:18255</a>             | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     |                     |
| CVE Program record  | CVE.ORG             | <a href="https://www.cve.org">www.cve.org</a>                 | canonical           |
| NVD vulnerability detail  | NVD                 | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               | 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)