Bug 2402142 (CVE-2025-11419) - CVE-2025-11419 keycloak: Keycloak TLS Client-Initiated Renegotiation Denial of Service

Keywords: Security

Status: NEW

Alias: CVE-2025-11419

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2025-10-07 11:17 UTC by OSIDB Bzimport

Modified: 2025-12-23 19:31 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-10-07 11:17:03 UTC Description

```
Keycloak is vulnerable to a Denial of Service (DoS) attack due
to the default JDK setting that permits Client-Initiated
Renegotiation in TLS 1.2. An unauthenticated remote attacker
can repeatedly initiate TLS renegotiation requests to exhaust
server CPU resources, making the service unavailable.
Immediate mitigation is available by setting the -
Djdk.tls.rejectClientInitiatedRenegotiation=true Java system
property in the Keycloak startup configuration.

Requirements to exploit

An attacker requires network access to any TLS-enabled
endpoint on a Keycloak server. No authentication is required
```

```
to launch the attack.
```

Note

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