CVE-2026-1180

VEX

Public on January 19, 2026

Last modified: April 2, 2026 at 1:56:51 PM UTC

MODERATE

Moderate severity

What does this mean?

5.8

CVSS v3 Score Breakdown

Jump to section

Description Statement Mitigation Additional information Affected Packages CVSS Score Details Weakness (CWE) Acknowledgements FAQ

Description

A flaw was identified in Keycloak’s OpenID Connect Dynamic Client Registration feature when clients authenticate using private_key_jwt. The issue allows a client to specify an arbitrary jwks_uri, which Keycloak then retrieves without validating the destination. This enables attackers to coerce the Keycloak server into making HTTP requests to internal or restricted network resources. As a result, attackers can probe internal services and cloud metadata endpoints, creating an information disclosure and reconnaissance risk.

Statement

This vulnerability is rated Moderate for Red Hat. The flaw in Keycloak's OIDC Dynamic Client Registration allows an attacker to force the Keycloak server to make requests to internal network resources via a crafted jwks_uri parameter. This can lead to information disclosure and internal n

etwork reconnaissance, particularly in configurations that permit anonymous or token-based cli ent registration.

Mitigation

Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Additional information

- Bugzilla 2430781: org.keycloak.protocol.oidc: Blind Server-Side Request Forgery (SSRF) in Keycloak OIDC Dynamic Client Registration via jwks_uri
- CWE-918: Server-Side Request Forgery (SSRF)

External references

- https://www.cve.org/CVERecord?id=CVE-2026-1180
- https://nvd.nist.gov/vuln/detail/CVE-2026-1180

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat build of Keycloak 26.4
Components	rhbk/keycloak-operator-bundle
State	Fixed
Justification	None
Errata	RHSA-2026:6478
Release Date	April 2, 2026

Products / Services	Red Hat build of Keycloak 26.4
Components	rhbk/keycloak-rhel9
State	Fixed
Justification	None
Errata	RHSA-2026:6478
Release Date	April 2, 2026

Products / Services	Red Hat build of Keycloak 26.4
Components	rhbk/keycloak-rhel9-operator
State	Fixed
Justification	None
Errata	RHSA-2026:6478

1 of 1

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	5.8	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	None	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Changed	N/A	N/A
Confidentiality Impact	Low	N/A	N/A
Integrity Impact	None	N/A	N/A
Availability Impact	None	N/A	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Acknowledgements

Red Hat would like to thank Lucas Montes (Nirox) for reporting this issue.

Frequently Asked Questions

- **Why is Red Hat's CVSS v3 score or Impact different from other vendors?**
- **My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?**
- **What can I do if my product is listed as "Will not fix"?**
- **What can I do if my product is listed as "Fix deferred"?**
- **What is a mitigation?**
- **I have a Red Hat product but it is not in the above list, is it affected?**
- **Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?**

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: April 2, 2026 at 1:56:51 PM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage