CVE-

VEX

Public on

Last modi

cription

ements

Descri

A flaw wa ak

accepts F

configura n

segments, potentially bypassing proxy-level path filtering. This could expose administrative or sensitive endpoints that operators believe are not externally reachable.

Statement

This vulnerability is rated Low for Red Hat Keycloak. The flaw arises from Keycloak's acceptance of RFC-compliant matrix parameters in URL paths, which can be mishandled by certain reverse proxy configurations. This may allow an unauthenticated attacker to bypass proxy-level path filtering and potentially expose administrative or sensitive endpoints that are intended to be unreachable externally. Exploitation depends on the specific reverse proxy configuration.

Mitigation

To mitigate this issue, ensure that all administrative and sensitive endpoints within Keycloak are adequately protected by robust authentication and authorization policies, independent of any reverse proxy path filtering. Operators should review Keycloak's internal access controls to confirm that access to these endpoints is restricted to authorized users and roles.

Additional information

- Bugzilla 2429869: org.keycloak/keycloak-quarkus-server: Keycloak: Proxy bypass due to improper handling of matrix parameters in URL paths
- CWE-20: Improper Input Validation

External references

- https://www.cve.org/CVERecord?id=CVE-2026-0976
- https://nvd.nist.gov/vuln/detail/CVE-2026-0976

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata

Clear all

Products / Services	Red Hat Build of Keycloak
Components	org.keycloak/keycloak-quarkus-server
State	Affected
Justification	None
Errata	
Release Date	

Products / Services	Red Hat JBoss Enterprise Application Platform 8
Components	keycloak-quarkus-server
State	Fix deferred
Justification	None
Errata	
Release Date	

Products / Services	Red Hat JBoss Enterprise Application Platform 8

1-10 of 7

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.

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).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	3.7	N/A
Attack Vector	Network	N/A
Attack Complexity	High	N/A

	Red Hat	NVD
Privileges Required	None	N/A
User Interaction	None	N/A
Scope	Unchanged	N/A
Confidentiality Impact	Low	N/A
Integrity Impact	None	N/A
Availability Impact	None	N/A

CVSS v3 Vector

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

Acknowledgements

Red Hat would like to thank Alexander Schwartz (RedHat) 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: January 15, 2026 at 12:06:16 PM UTC

Red Hat Summit