CVE-

VEX
Public on
Last mod

Jump to section

Description

A flaw was found in Keycloak. The Keycloak Authorization header parser is overly permissive regarding the formatting of the "Bearer" authentication scheme. It accepts non-standard characters (such as tabs) as separators and tolerates case variations that deviate from RFC 6750 specifications.

Statement

This vulnerability is rated Moderate for Red Hat because Keycloak's excessive tolerance for non-standard Bearer token formats in the Authorization header can lead to inconsistencies with front-end security controls such as WAFs and proxies. This may enable potential bypass risks, allowing malformed tokens to circumvent intended security policies.

Mitigation

To mitigate this issue, configure any front-end security controls, such as Web Application Firewalls (WAFs) or reverse proxies, to strictly validate and normalize the `Authorization` header before forwarding requests to Keycloak. This ensures that only standard Bearer token formats are processed, preventing potential bypasses.

Additional information

- Bugzilla 2427768: keycloak: Keycloak Authorization Header Parsing Leading to Potential Security Control Bypass
- CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization

External references

- https://www.cve.org/CVERecord?id=CVE-2026-0707
- https://nvd.nist.gov/vuln/detail/CVE-2026-0707

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	5.3	N/A
Attack Vector	Network	N/A
Attack Complexity	Low	N/A

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

CVSS v3 Vector

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

Acknowledgements

Red Hat would like to thank Guanping Zhang 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 8, 2026 at 3:41:22 AM UTC