CVE-2024-8698

VEX

Public on September 19, 2024

Last modified: October 3, 2025 at 12:41:22 PM UTC

IMPORTANT

Important severity

What does this mean?

7.7

CVSS v3 Score Breakdown

Jump to section

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

Description

A flaw exists in the SAML signature validation method within the Keycloak XMLSignatureUtil class. The method incorrectly determines whether a SAML signature is for the full document or only for specific assertions based on the position of the signature in the XML document, rather than the Reference element used to specify the signed element. This flaw allows attackers to create crafted responses that can bypass the validation, potentially leading to privilege escalation or impersonation attacks.

Statement

This vulnerability is of high severity due to its potential to facilitate privilege escalation and user impersonation in systems using SAML for authentication. The core issue stems from improper v alidation logic in Keycloak's signature validation method, which relies on the position of signatur

es rather than explicitly checking the referenced elements. By manipulating the XML structure, an attacker can bypass signature validation and inject an unsigned assertion while retaining a val id signed one. This allows unauthorized access to high-privileged accounts, leading to significan t security risks in SAML-based identity providers and service providers.

Mitigation

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

Additional information

- Bugzilla 2311641: keycloak-saml-core: Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak
- CWE-347: Improper Verification of Cryptographic Signature
- FAQ: Frequently asked questions about CVE-2024-8698

External references

- https://www.cve.org/CVERecord?id=CVE-2024-8698
- https://nvd.nist.gov/vuln/detail/CVE-2024-8698

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
Components	
State	Fixed
Justification	None
Errata	RHSA-2024:6888
Release Date	September 19, 2024

Products / Services	Red Hat Build of Keycloak
Components	org.keycloak/keycloak-saml-core
State	Fixed
Justification	None
Errata	RHSA-2024:6890
Release Date	September 19, 2024

Products / Services	Red Hat build of Keycloak 22
Components	rhbk/keycloak-operator-bundle
State	Fixed
Justification	None
Errata	RHSA-2024:6887

1 of 10

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	7.7	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	High	N/A	N/A
Privileges Required	Low	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Changed	N/A	N/A
Confidentiality Impact	High	N/A	N/A
Integrity Impact	Low	N/A	N/A
Availability Impact	Low	N/A	N/A

CVSS v3 Vector

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

Acknowledgements

Red Hat would like to thank Tanner Emek 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: October 3, 2025 at 12:41:22 PM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

All systems operational