CVE

VEX

Public or

Last mod

Jump to section

Description

A flaw was found in Tempo Operator, where it creates a ServiceAccount, ClusterRole, and ClusterRoleBinding when a user deploys a TempoStack or TempoMonolithic instance. This flaw allows a user with full access to their namespace to extract the ServiceAccount token and use it to submit TokenReview and SubjectAccessReview requests, potentially revealing information about other users' permissions. While this does not allow privilege escalation or impersonation, it exposes information that could aid in gathering information for further attacks.

Statement

Red Hat has evaluated this vulnerability and rated with a Moderate impact as the attacker is limited to read access and requires previous permissions to read the token and get access to the cluster metrics.

Mitigation

Currently, no mitigation is available for this vulnerability.

Additional information

- Bugzilla 2354811: tempo-operator: ServiceAccount Token Exposure Leading to Token and Subject Access Reviews in OpenShift Tempo Operator
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

External references

- https://www.cve.org/CVERecord?id=CVE-2025-2786
- https://nvd.nist.gov/vuln/detail/CVE-2025-2786

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat OpenShift distributed tracing 3.5.1
Components	rhosdt/tempo-rhel8-operator

State	Fixed
Justification	None
Errata	RHSA-2025:3607
Release Date	April 4, 2025

Products / Services	Red Hat OpenShift distributed tracing 3.5.1
Components	rhosdt/tempo-rhel8-operator
State	Fixed
Justification	None
Errata	RHSA-2025:3740
Release Date	April 9, 2025

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).

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	4.3	N/A
Attack Vector	Network	N/A
Attack Complexity	Low	N/A
Privileges Required	Low	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:L/PR:L/UI:N/S:U/C:L/I:N/A:N

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: September 26, 2025 at 11:57:29 AM UTC

Quick Links

Help

Site Info

Related Sites

All systems operational