CVE

VEX

Public or

Last mod

Jump to section

Description

A flaw was found in Podman. In a Containerfile or Podman, data written to RUN --mount=type=bind mounts during the podman build is not discarded. This issue can lead to files created within the container appearing in the temporary build context directory on the host, leaving the created files accessible.

Statement

This issue is classified as Moderate rather than Important because exploitation requires several preconditions: an attacker must have unprivileged access to the host during the build process, the container build must include long-running steps (e.g., RUN sleep) that prolong

the existence of the temporary build context, and files must be created with overly permissive permissions (e.g., 4777). The vulnerability does not allow remote code execution or compromise of running containers, and it only exposes files temporarily present in the build context. Therefore, while it can lead to information disclosure, the scope and impact are limited to local users with concurrent access, making the overall risk moderate.

Mitigation

Avoid long-running build steps and overly permissive file permissions. Use RUN --mount=type=secret for sensitive data instead of bind mounts.

Additional information

- Bugzilla 2367235: podman: Build Context Bind Mount
- CWE-378: Creation of Temporary File With Insecure Permissions

External references

- https://www.cve.org/CVERecord?id=CVE-2025-4953
- https://nvd.nist.gov/vuln/detail/CVE-2025-4953
- https://github.com/containers/podman/pull/25173

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Enterprise Linux 8

Components	container-tools:rhel8
State	Fixed
Justification	None
Errata	RHSA-2025:15904
Release Date	September 16, 2025

Products / Services	Red Hat OpenShift Container Platform 4.12
Components	podman
State	Fixed
Justification	None
Errata	RHSA-2025:17669
Release Date	October 16, 2025

1-10 of 33

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	7.4	N/A
Attack Vector	Network	N/A
Attack Complexity	High	N/A
Privileges Required	None	N/A
User Interaction	None	N/A
Scope	Unchanged	N/A
Confidentiality Impact	High	N/A
Integrity Impact	High	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:H/I:H/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: November 10, 2025 at 1:54:43 PM UTC

Quick Links

Help

Site Info

Related Sites

All systems operational

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit