CVE

VEX

Public or

Last moc

Description ments FAQ

Descr

There's

overwrit nt and

such vol ker can

only cor.. le.

Binary-Affected: podman Upstream-version-introduced: v4.0.0 Upstream-version-fixed: v5.6.1

Statement

The Red Hat Product Security team has evaluated this vulnerability as having the Important sev erity. This happens because of the consequences of an successful attack and the low complexit y (AC:L) on exploiting this vulnerability. Although the attacker cannot control the content writte

n to the target file, depending on which file was targeted, the exploitation of this flaw may lead sensitive data corruption (I:H) and leading the system to crash resulting in a Denial of Service at tack (A:H).

Mitigation

Red Hat advises to not run the podman kube play command with untrusted Kubernetes YAML file as input, additionally review the Kubernetes YAML file before running it through podman may help to catch maliciously crafted secretes or volumes that may be used to exploit this vulnerability.

Additional information

- Bugzilla 2393152: podman: Podman kube play command may overwrite host files
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

External references

- https://www.cve.org/CVERecord?id=CVE-2025-9566
- https://nvd.nist.gov/vuln/detail/CVE-2025-9566
- https://github.com/containers/podman/commit/43fbde4e665fe6cee6921868f04b7ccd3de5ad89
- https://github.com/containers/podman/security/advisories/GHSA-wp3j-xq48-xpjw

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 Enterprise Linux 10
Components	podman
State	Fixed
Justification	None
Errata	RHSA-2025:15901
Release Date	September 16, 2025

Products / Services	Red Hat Enterprise Linux 10
Components	podman
State	Fixed
Justification	None
Errata	RHSA-2025:20983
Release Date	November 11, 2025

Products / Services	Red Hat Enterprise Linux 8
Components	container-tools:rhel8
State	Fixed
Justification	None
Errata	RHSA-2025:15904

1 of 36

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

CVSS v3 Vector

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

Acknowledgements

This issue was discovered by Paul Holzinger (Red Hat).

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: March 19, 2026 at 5:24:59 PM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage