



CVE

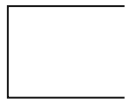
Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



VEX

Public or

Last mod



A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Descr

There's

overwrit

such vol

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy settings, then we recognize the global privacy settings from your browser.

only control the target file to be overwritten but not the content to be written into the file.

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 severity. This happens because of the consequences of a successful attack and the low complexity (AC:L) on exploiting this vulnerability. Although the attacker cannot control the content written

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 attack (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 secrets 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
CVE description copyright © 2021



Quick Links



Help



Site Info



Related Sites



 Partial system outage



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Opt-Out Rights](#)