About cookies on this site

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 cross-context

Accept Default

Do Not Sell or Share My Personal Information

Red Hat P

RHSA

024-11-12

Overview

Updated Pa

Synop

Moderat

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update for podman is now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

Description

The podman tool manages pods, container images, and containers. It is part of the libpod library, which is for applications that use container pods. Container pods is a concept in Kubernetes.

Security Fix(es):

- podman: Symlink error leads to information disclosure (CVE-2022-4122)
- containers/image: digest type does not guarantee valid type (CVE-2024-3727)
- golang: archive/zip: Incorrect handling of certain ZIP files (CVE-2024-24789)
- net/http: Denial of service due to improper 100-continue handling in net/http (CVE-2024-24791)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 9.5 Release Notes linked from the References section.

Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

Affected Products

- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x

Fixes

- BZ - 2144983 - CVE-2022-4122 podman: Symlink error leads to information disclosure
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2292668 - CVE-2024-24789 golang: archive/zip: Incorrect handling of certain ZIP files

- BZ - 2295310 - CVE-2024-24791 net/http: Denial of service due to improper 100-continue handling in net/http
- RHEL-29763 - Update podman to new upstream release in 9.5
- RHEL-24333 - [RFE] podman 5: to edit the information under man containers.conf
- RHEL-27171 - [RFE] podman 5: Add configurability to Netavark firewall driver
- RHEL-17776 - podman 5: Unable to copy image from one virtual machine to another using "podman image scp"
- RHEL-3092 - [podman-5.2][RFE] podman 5: Option to name network interface inside container same as the respective podman network interface name of its parent by default
- RHEL-32599 - podman 5 is actually 4.9.3-dev
- RHEL-28803 - podman image mount issue when additional image stores are used
- RHEL-18987 - [podman5.1] Configurable logging for Podman healthcheck events
- RHEL-48917 - [Rebase] podman 5 for nftables support
- RHEL-48760 - [podman-5.2] Unable to run "podman system renumber"
- RHEL-40811 - [podman-5.2] Listing tags in JFrog Artifactory may fail - Podman RHEL 9.5
- RHEL-45979 - [podman-5.2] podman system reset doesn't remove blob-info-cache-v1.sqlite
- RHEL-54361 - podman container with --userns=keep-id doesn't respect restart policy

CVEs

- CVE-2022-4122
- CVE-2024-3727
- CVE-2024-24789
- CVE-2024-24791

References

- https://access.redhat.com/security/updates/classification/#moderate
- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/9.5_release_notes/index

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Loading

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 Do Not Sell or Share My Personal Information