RHSA-2024:9459 - Security Advisory

Issued: 2024-11-12 Updated: 2024-11-12

Overview

Updated Packages

Synopsis

Important: buildah security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

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

Red Hat Product Security has rated this update as having a security impact of Important. 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 buildah package provides a tool for facilitating building OCI container images. Among other things, buildah enables you to: Create a working container, either from scratch or using an image as a starting point; Create an image, either from a working container or using the instructions in a Dockerfile; Build both Docker and OCI images.

Security Fix(es):

- go/parser: golang: Calling any of the Parse functions containing deeply nested literals can cause a panic/stack exhaustion (CVE-2024-34155)
- encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion (CVE-2024-34156)
- go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion (CVE-2024-34158)
- Podman: Buildah: cri-o: FIPS Crypto-Policy Directory Mounting Issue in containers/common Go Library (CVE-2024-9341)
- Buildah: Podman: Improper Input Validation in bind-propagation Option of Dockerfile RUN --mount Instruction (CVE-2024-9407)
- buildah: Buildah allows arbitrary directory mount (CVE-2024-9675)
- Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS) (CVE-2024-9676)

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.

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 - 2310527 - CVE-2024-34155 go/parser: golang: Calling any of the Parse functions containing deeply nested literals can cause a panic/stack exhaustion
- BZ - 2310528 - CVE-2024-34156 encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion
- BZ - 2310529 - CVE-2024-34158 go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion
- BZ - 2315691 - CVE-2024-9341 Podman: Buildah: cri-o: FIPS Crypto-Policy Directory Mounting Issue in containers/common Go Library
- BZ - 2315887 - CVE-2024-9407 Buildah: Podman: Improper Input Validation in bind-propagation Option of Dockerfile RUN --mount Instruction
- BZ - 2317458 - CVE-2024-9675 buildah: Buildah allows arbitrary directory mount
- BZ - 2317467 - CVE-2024-9676 Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS)
- RHEL-62107 - Buildah in RHEL 9.5 is built without CNI support - [RHEL-9.5 0day]

CVEs

- CVE-2024-9341
- CVE-2024-9407
- CVE-2024-9675
- CVE-2024-9676
- CVE-2024-34155
- CVE-2024-34156
- CVE-2024-34158

References

- https://access.redhat.com/security/updates/classification/#important

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