Red Hat F

RHSA

:4-11-08

Overview

Updated P

Synop

Importa

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

Red Hat OpenShift Container Platform release 4.14.40 is now available with updates to packages and images that fix several bugs and add enhancements.

This release includes a security update for Red Hat OpenShift Container Platform 4.14.

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

Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.

This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.14.40. See the following advisory for the container images for this release:

https://access.redhat.com/errata/RHSA-2024:8697

Security Fix(es):

- buildah: Buildah allows arbitrary directory mount (CVE-2024-9675)
- 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)

- Podman: Buildah: CRI-O: symlink traversal vulnerability in the

containers/storage library can cause Denial of Service (DoS) (CVE-2024-9676)

- go/parser: golang: Calling any of the Parse functions containing deeply

nested literals can cause a panic/stack exhaustion (CVE-2024-34155)

- 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)

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.

All OpenShift Container Platform 4.14 users are advised to upgrade to these updated packages and images when they are available in the appropriate release channel. To check for available updates, use the OpenShift CLI (oc) or web console. Instructions for upgrading a cluster are available at https://docs.openshift.com/container-platform/4.14/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.14 see the following documentation, which will be updated shortly for this release, for important instructions on how to upgrade your cluster and fully apply this asynchronous errata update:

https://docs.openshift.com/container-platform/4.14/release_notes/ocp-4-14-release-notes.html

Affected Products

- Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64

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 - 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)

CVEs

- 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/.

Red Hat

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility