RHSA-2025:2454 - Security Advisory

Issued: 2025-03-13 Updated: 2025-03-13

Synopsis

Important: OpenShift Container Platform 4.15.47 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.15.47 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 4.15.

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 container images for Red Hat OpenShift Container Platform 4.15.47. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2025:2456

Space precludes documenting all of the container images in this advisory. See the following Release Notes documentation, which will be updated shortly for this release, for details about these changes:

https://docs.openshift.com/container-platform/4.15/release_notes/ocp-4-15-release-notes.html

Security Fix(es):

- buildah: Buildah allows arbitrary directory mount (CVE-2024-9675)
- bind: bind9: Many records in the additional section cause CPU exhaustion

(CVE-2024-11187)

- podman: buildah: Container breakout by using --jobs=2 and a race

condition when building a malicious Containerfile (CVE-2024-11218)

- kernel: HID: core: zero-initialize the report buffer (CVE-2024-50302)
- 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. All OpenShift Container Platform 4.15 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/4.15/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.15 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/4.15/release_notes/ocp-4-15-release-notes.html

You may download the oc tool and use it to inspect release image metadata for x86_64, s390x, ppc64le, and aarch64 architectures. The image digests may be found at https://quay.io/repository/openshift-release-dev/ocp-release?tab=tags.

The sha values for the release are as follows:

(For x86_64 architecture)
The image digest is
sha256:5b4a7992e54844ee8614476993919b7cd2d7d21dd3a48daaacf7a9c4f17bece6

(For s390x architecture)
The image digest is
sha256:022a3666b20cb12d5b907fb0025ee2ca0101b632dd8bc7851746f3fd409c3559

(For ppc64le architecture)
The image digest is
sha256:28a99ce4052c87e3b88ca80da191a61f058e3b8735b7437b6c4b0ffb9e360371

(For aarch64 architecture)
The image digest is
sha256:0ecfd307bd4e9ac0b218ea79f419cb78d7e88ead502e33724aa91b8ab041f497

All OpenShift Container Platform 4.15 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/4.15/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.15 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.15 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 8 aarch64

Fixes

- 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)
- BZ - 2326231 - CVE-2024-11218 podman: buildah: Container breakout by using --jobs=2 and a race condition when building a malicious Containerfile
- BZ - 2327169 - CVE-2024-50302 kernel: HID: core: zero-initialize the report buffer
- BZ - 2342879 - CVE-2024-11187 bind: bind9: Many records in the additional section cause CPU exhaustion

- OCPBUGS-41614 - 4.15: Disable:Broken for [sig-builds][Feature:Builds][Slow] can use private repositories as build input build using an HTTP token should be able to clone source code via an HTTP token [apigroup:build.openshift.io]
- OCPBUGS-42970 - [release-4.15] Collect number of resources in etcd by must-gather
- OCPBUGS-43605 - Allow from host network networkpolicies do not work during live migration
- OCPBUGS-44657 - add IBM Block Storage CSI driver support for RWX
- OCPBUGS-48473 - [release-4.15] failed to provision volume with StorageClass "thin-csi-default"
- OCPBUGS-48749 - [openshift-4.15] OWNERS update for build componet
- OCPBUGS-49647 - [openshift-4.15] CI Failure: [sig-builds][Feature:Builds][Slow] s2i build with environment file in sources Building from a template should create a image from "test-env-build.json" template and run it in a pod
- OCPBUGS-49849 - [release-4.15] Silenced alert seen on openshift console overview page
- OCPBUGS-51253 - Pods cannot connect to apiserver in IPv6 disconnected hosted cluster
- OCPBUGS-51332 - [release-4.16] After upgrading the cluster to 4.15 the Prometheus Operator?s "Prometheus" tab does not show the Prometheuses
- OCPBUGS-52172 - Cluster fails to complete provisioning when using proxy with custom trust bundle

CVEs

- CVE-2024-9675
- CVE-2024-9676
- CVE-2024-11187
- CVE-2024-11218
- CVE-2024-50302
- CVE-2025-1094
- CVE-2025-1244

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

Loading

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit