RHSA-2025:0876 - Security Advisory

Issued: 2025-02-05 Updated: 2025-02-05

Synopsis

Moderate: OpenShift Container Platform 4.17.15 bug fix and security update

Type/Severity

Security Advisory: Moderate

Topic

Red Hat OpenShift Container Platform release 4.17.15 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 4.17.

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

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 4.17.15. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2025:0878

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/4.17/release_notes/ocp-4-17-release-notes.html

Security Fix(es):

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

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

- path-to-regexp: path-to-regexp Unpatched `path-to-regexp` ReDoS in 0.1.x

(CVE-2024-52798)

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 4.17 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/4.17/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.17 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/4.17/release_notes/ocp-4-17-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
sha256:68ffa083a5ab473d9fd87cedcb01c6f27740aad92de0ee39a7ac408da9a65857

(For s390x architecture)
The image digest is
sha256:846ebc62ab2f2f449260b34d16a40f070c43b29a4d79455796e8aa700453dc97

(For ppc64le architecture)
The image digest is
sha256:1176732e9041adc188c006da5e3bb77cf7b90c5fd85ee6ab0390c91cbf8a7e0c

(For aarch64 architecture)
The image digest is
sha256:1a6db02e197341338e207a850b4a12cf2ab3e1e4fda8ed72b563051e57b4a8fa

All OpenShift Container Platform 4.17 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/4.17/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.17 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.17 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.17 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.17 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 8 aarch64

Fixes

- BZ - 2317467 - CVE-2024-9676 Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS)
- BZ - 2330689 - CVE-2024-52798 path-to-regexp: path-to-regexp Unpatched `path-to-regexp` ReDoS in 0.1.x
- OCPBUGS-43751 - Do not have access to token when make request using devconsole proxy
- OCPBUGS-44220 - Enable knative e2e tests in CI
- OCPBUGS-47801 - Multiple reboots during EUS upgrade on Control Plane nodes
- OCPBUGS-48257 - [IBMCloud] remove the VM type which test failed from tested_instance_types
- OCPBUGS-48645 - Azure: installer sometimes fails to provision control plane
- OCPBUGS-48691 - ClusterResourceOverride operator fails to reconcile the clusterresourceoverride-configuration configMap

- OCPBUGS-48695 - OLMv0: excessive catalog source snapshots cause severe performance regression [openshift-4.17.z]
- OCPBUGS-48704 - The name proposed by the UI for a new service is `exampleasd`
- OCPBUGS-48745 - <4.17>Whereabouts kubeconfig known to expire
- OCPBUGS-49350 - static IP manager crashloops for a while on pod startup
- OCPBUGS-49362 - [Nutanix] Installation failed with timeout when uploading images to PC
- OCPBUGS-49411 - Etcd quorum lost during bootstrap because two static pod installers trigger concurrent rollouts - 4.17
- OCPBUGS-49650 - Topology view crashes

CVEs

- CVE-2024-9676
- CVE-2024-12085
- CVE-2024-52531
- CVE-2024-52798
- CVE-2024-53263

References

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

---

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

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
Cookie preferences