RHSA-2024:6818 - Security Advisory

Issued: 2024-09-25 Updated: 2024-09-25

Overview

Updated Images

Synopsis

Moderate: OpenShift Container Platform 4.15.34 bug fix and security update

Type/Severity

Security Advisory: Moderate

Topic

Red Hat OpenShift Container Platform release 4.15.34 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 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 4.15.34. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHBA-2024:6821

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):

- QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server

During Socket Closure (CVE-2024-7409)

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:

(For x86_64 architecture)
The image digest is
sha256:f2e0c593f6ed81250c11d0bac94dbaf63656223477b7e8693a652f933056af6e

(For s390x architecture)
The image digest is
sha256:357949b571429fc187fd9f80766ca730de2b8fe35b0bfd10a604958a1756c754

(For ppc64le architecture)
The image digest is
sha256:e95ac38bd9f3189f2f4acaf19e10c10ad5f01ac9921e54b418410441ed927eb0

(For aarch64 architecture)
The image digest is
sha256:4fb3b9374aa74dea5e568d584fc3f09220ffd9a70f4c39eb11d822a69d647220

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 - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- OCPBUGS-35869 - ocm-operator: panic detected in pod
- OCPBUGS-35922 - lots of churn during image registry managed/removed transition
- OCPBUGS-37464 - [4.15.z] SCC pinning for all workloads in platform namespaces (cluster-samples-operator)
- OCPBUGS-37727 - Backport owners file for multus admission controller
- OCPBUGS-38065 - [release-4.15] LDAP communication going through HTTP(S) proxy
- OCPBUGS-38108 - Cannot create web-terminals as kubeadmin on OpenShift 4.15+
- OCPBUGS-38593 - [release4.15] IO Enhancement: Start collecting haproxy_exporter_server_threshold metric
- OCPBUGS-41340 - [4.15] EgressIP intermittent connection timeout while communicating with external services
- OCPBUGS-41598 - [FLAKE] e2e: upgrade CRD with deprecated version
- OCPBUGS-41635 - [Backport-4.15] Cluster-ingress-operator logs an update when one didn't happen
- OCPBUGS-41701 - The hypershift cli (hcp) reports an inaccurate OCP supported version
- OCPBUGS-41809 - [4.15] AdditionalTrustedCA in ImageConfig is not wired correctly
- OCPBUGS-41819 - [4.15] Install plan is unable to move forward and is stuck in Pending state when the amount of CRs is too high.

- OCPBUGS-41946 - Cloud Event API GET CurrentState has extra '/' in ResourceAddress
- OCPBUGS-41947 - HCP: nodes never become available when workers require a proxy to access KAS
- OCPBUGS-41981 - [4.15]OLM catalogsource pods do not recover from node failure when registryPoll is none

CVEs

- CVE-2023-52880
- CVE-2024-3727
- CVE-2024-6602
- CVE-2024-7409
- CVE-2024-26886
- CVE-2024-26974
- CVE-2024-38559
- CVE-2024-38573
- CVE-2024-38615
- CVE-2024-40984
- CVE-2024-41023
- CVE-2024-41031
- CVE-2024-42241
- CVE-2024-42243
- CVE-2024-42246

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

Loading