RHSA-2024:8991 - Security Advisory

Issued: 2024-11-13 Updated: 2024-11-13

Synopsis

Important: OpenShift Container Platform 4.15.38 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.15.38 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 4.15.38. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2024:8994

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):

- openshift-console: OAuth2 insufficient state parameter entropy

(CVE-2024-6508)

- dompurify: nesting-based mutation XSS vulnerability (CVE-2024-47875)
- opentelemetry: DoS vulnerability in otelhttp (CVE-2023-45142)
- 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 as follows:

(For x86_64 architecture)
The image digest is
sha256:bcc1b1803a49b9ac876a7dd950138439aacb81f070a64ae0a2f16e01594b7291

(For s390x architecture)
The image digest is
sha256:a30a4b62995d123fd352ca1676847414e55c7728b23655435d5fce4227d6a486

(For ppc64le architecture)
The image digest is
sha256:f8d27d42b75c58ae8bf89820ee089893fdeeebfe6b80dd0481994da9e9c6c7a0

(For aarch64 architecture)
The image digest is
sha256:16f31d7b926ce2bdae0e4bf911fffb68d30b449870c99c6411c9ecc0648d7b91

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 - 2245180 - CVE-2023-45142 opentelemetry: DoS vulnerability in otelhttp
- BZ - 2295777 - CVE-2024-6508 openshift-console: OAuth2 insufficient state parameter entropy
- BZ - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- BZ - 2318052 - CVE-2024-47875 dompurify: nesting-based mutation XSS vulnerability
- OCPBUGS-30207 - --destroy-cloud-resources does not work for HCP KubeVirt platform
- OCPBUGS-34510 - Migrate HyperShift KAS to none endpoint reconciler type
- OCPBUGS-42110 - Node sclaling failed due to misconfigurations in on-prem-resolv-prepender.service in RHOCP4
- OCPBUGS-42865 - Built-in join subnet "100.64.0.0/16" overlaps cluster subnet "100.64.0.0/15" even though internalJoinSubnet is configured
- OCPBUGS-42930 - Continuous pull-secret updates / slow initialization on build01 (test platform infrastructure)
- OCPBUGS-43268 - CNO must report status while deploying IPsec

- OCPBUGS-43575 - MCPs report wrong number of nodes when we move nodes from one custom MCP to another custom MCP
- OCPBUGS-43582 - Panic seen in CI job for MCC pod
- OCPBUGS-43646 - [4.15] Cloud Credentials operator generating millions of messages per day in GCP clusters
- OCPBUGS-43656 - Image registry operator becomes degraded when setting management state to Removed when networkAccess is set to Internal
- OCPBUGS-43855 - 4.15+ Cloud Credential Operator down due to GCP backupdr.googleapis.com access request
- OCPBUGS-43876 - Missing runbook for the TelemeterClientFailures alerting rule
- OCPBUGS-43918 - Fix TestOperandProxyConfiguration and TestLeaderElection flakes on Image Registry Operator
- OCPBUGS-44035 - [IBMCloud] install only checks first set of subnets (no pagination support)
- OCPBUGS-44201 - OIDC IDP validation check should not be fatal to CPO reconcilation

CVEs

- CVE-2019-12900
- CVE-2022-48773
- CVE-2022-48936
- CVE-2023-45142
- CVE-2023-52492
- CVE-2024-2314
- CVE-2024-3596
- CVE-2024-6508
- CVE-2024-7006
- CVE-2024-7409
- CVE-2024-9341
- CVE-2024-9675
- CVE-2024-9676
- CVE-2024-24857
- CVE-2024-26851
- CVE-2024-26924
- CVE-2024-26976
- CVE-2024-27017
- CVE-2024-27062
- CVE-2024-34155
- CVE-2024-34156
- CVE-2024-34158
- CVE-2024-35839
- CVE-2024-35898

- CVE-2024-35939
- CVE-2024-38540
- CVE-2024-38541
- CVE-2024-38586
- CVE-2024-38608
- CVE-2024-39503
- CVE-2024-40924
- CVE-2024-40961
- CVE-2024-40983
- CVE-2024-40984
- CVE-2024-41009
- CVE-2024-41042
- CVE-2024-41066
- CVE-2024-41092
- CVE-2024-41093
- CVE-2024-42070
- CVE-2024-42079
- CVE-2024-42244
- CVE-2024-42284
- CVE-2024-42292
- CVE-2024-42301
- CVE-2024-43854
- CVE-2024-43880
- CVE-2024-43889
- CVE-2024-43892
- CVE-2024-44935
- CVE-2024-44989
- CVE-2024-44990
- CVE-2024-45018
- CVE-2024-46826
- CVE-2024-47668
- CVE-2024-47875

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