RHSA-2024:6824 - Security Advisory

Issued: 2024-09-24 Updated: 2024-09-24

Synopsis

Moderate: OpenShift Container Platform 4.16.14 security update

Type/Severity

Security Advisory: Moderate

Topic

Red Hat OpenShift Container Platform release 4.16.14 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 4.16.

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.
Security Fix(es):

- containers/image: digest type does not guarantee valid type

(CVE-2024-3727)

- golang-protobuf: encoding/protojson, internal/encoding/json: infinite

loop in protojson.Unmarshal when unmarshaling certain forms of invalid JSON
(CVE-2024-24786)

- Bare Metal Operator: BMO can expose particularly named secrets from other

namespaces via BMH CRD (CVE-2024-43803)

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.

Solution

For OpenShift Container Platform 4.16 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/4.16/release_notes/ocp-4-16-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
sha256:0521a0f1acd2d1b77f76259cb9bae9c743c60c37d9903806a3372c1414253658

(For s390x architecture)
The image digest is
sha256:10935ec4eff66bc610801300a4376e6d733631e93681ef1dae5f0962fec98681

(For ppc64le architecture)
The image digest is
sha256:dbf7aec1bd0a24fd5a23d6ac927d101b7e0cfcb8d4ccb8c440b2ed17a0dd9705

(For aarch64 architecture)
The image digest is
sha256:76eb80594e33fc9300a0f36e4402e5232681eddf948b995a8d1acfd2fc7d72f9

All OpenShift Container Platform 4.16 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/4.16/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.16 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 9 aarch64

Fixes

- BZ - 2268046 - CVE-2024-24786 golang-protobuf: encoding/protojson, internal/encoding/json: infinite loop in protojson.Unmarshal when unmarshaling certain forms of invalid JSON
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- BZ - 2309536 - CVE-2024-43803 Bare Metal Operator: BMO can expose particularly named secrets from other namespaces via BMH CRD
- OCPBUGS-24386 - VRF integration does not work when external traffic policy is local
- OCPBUGS-34518 - Local development: User toggle is not visible when authentification is disabled
- OCPBUGS-36855 - Openstack UPI - Reintroduce unique resource names
- OCPBUGS-37046 - Topology view shows "TypeError: Cannot read properties of null (reading 'metadata')"
- OCPBUGS-37763 - iptables-alerter logs spurious events under heavy load
- OCPBUGS-37937 - HCP: nodes never become available when workers require a proxy to access KAS
- OCPBUGS-38021 - [release-4.16] Integrate openstack related CRs with insights-operator
- OCPBUGS-38058 - [release-4.16] Hosted control planes: IDP communication through Konnectivity does not respect outgoing HTTP/s PROXY in DataPlane
- OCPBUGS-38502 - Power VS: Madrid cannot use e980 as a system type
- OCPBUGS-38911 - Values entered into the Instantiate Template form are automatically cleared

- OCPBUGS-39082 - vsphere - when folder is undefined and datacenter is in a folder, entire folder path is incorrectly created
- OCPBUGS-39179 - Prometheus no longer accepts samples of the same series with different timestamps
- OCPBUGS-39287 - UPI playbook failing due to missing metadata.json
- OCPBUGS-39496 - [AWS CAPI install] Network setting is not correct while install cluster into VPC which contains multi-CIDR subnets
- OCPBUGS-41540 - [4.16] opm creates FBCs which are incompatible with IIB catalogs
- OCPBUGS-41555 - SingleReplica HCPs can not upgrade on cluster with nodes in a single zone
- OCPBUGS-41619 - After updating the cluster to openshift 4.15.11 the value for vCenter Cluster in vsphere connnection configuration is missing.
- OCPBUGS-41677 - [4.16] Install plan is unable to move forward and is stuck in Pending state when the amount of CRs is too high.
- OCPBUGS-41806 - When newly built images rolled out, the update progress is not displaying correctly (went 0 --> 3)
- OCPBUGS-41886 - Cloud Event API GET CurrentState has extra '/' in ResourceAddress
- OCPBUGS-41910 - Alerts with a non-standard severity label should be filtered out from Telemetry

CVEs

- CVE-2023-52880
- CVE-2024-3727
- CVE-2024-24786
- 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
- CVE-2024-43803

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/.