RHSA
Advis
Overview
Updated Ir
Synop
Moderat
Type/
Security
Topic
Red Hat
images t
This rele
Red Hat
Vulnerab
for each

4-07-24

ges and

Common
ailable

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

https://access.redhat.com/errata/RHSA-2024:4616

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/4.16/release_notes/ocp-4-16-release-notes.html

Security Fix(es):

- ssh: Prefix truncation attack on Binary Packet Protocol (BPP)

(CVE-2023-48795)

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

(CVE-2024-3727)

- go-retryablehttp: url might write sensitive information to log file

(CVE-2024-6104)

- openssh: Possible remote code execution due to a race condition in signal

handling affecting Red Hat Enterprise Linux 9 (CVE-2024-6409)

- golang: net: malformed DNS message can cause infinite loop

(CVE-2024-24788)

- golang: net/netip: Unexpected behavior from Is methods for IPv4-mapped

IPv6 addresses (CVE-2024-24790)

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 4.16 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

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
sha256:633d1d36e834a70baf666994ef375b9d1702bd1c54ab46f96c41223af9c2d150

(For s390x architecture)
The image digest is
sha256:3acd5a5030ccf39daf86d1109c3aa00f1f48d5f62054a37c779e7c62178468ad

(For ppc64le architecture)
The image digest is
sha256:0d92c8189470fa0031c85e8f77e24d780ab3da4313b6454e88ad3bec909f269b

(For aarch64 architecture)
The image digest is
sha256:c853f47f5e8f8d8afb943f5a75757b6870c0b8bcf4507a1bbe4ad53e9ef3fdd6

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 - 2254210 - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2279814 - CVE-2024-24788 golang: net: malformed DNS message can cause infinite loop

- BZ - 2292787 - CVE-2024-24790 golang: net/netip: Unexpected behavior from Is methods for IPv4-mapped IPv6 addresses
- BZ - 2294000 - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- BZ - 2295085 - CVE-2024-6409 openssh: Possible remote code execution due to a race condition in signal handling affecting Red Hat Enterprise Linux 9
- OCPBUGS-32887 - OCP upgrade from 4.13 to 4.14 triggers the error "failed to update canary route openshift-ingress-canary/canary"
- OCPBUGS-34012 - Reduce the number of calls to the subscriptions fetchOrganization endpoint from console-operator
- OCPBUGS-35303 - kubelet-bootstrap-kubeconfig should have ownership annotations
- OCPBUGS-35310 - Listing tags in JFrog Artifactory may fail - Skopeo OCP 4.16
- OCPBUGS-35311 - Listing tags in JFrog Artifactory may fail - Podman OCP 4.16
- OCPBUGS-35836 - multus-admission-controller does not preserve modified resource requests/limits
- OCPBUGS-35864 - Metallb FRR-K8s: frr-k8s daemonset using quay.io/metallb/frr-k8s image
- OCPBUGS-36147 - [4.16] Resizing LUKS on 512e disk causes ignition-ostree-growfs to fail with "Device size is not aligned to requested sector size."
- OCPBUGS-36317 - PowerVS: Liveness probe error
- OCPBUGS-36450 - [4.16] Can't install operator on 4.15 after uninstalling it on a prior version
- OCPBUGS-36463 - etcd data store is leftover when infrastructure provisioning fails
- OCPBUGS-36673 - [4.16] Firmware Update causes BMH to get stuck in Preparing
- OCPBUGS-36704 - PTP operator showing high cpu utilization with steady workload on OCP 4.15
- OCPBUGS-36720 - [AWS] install failed with featureSet CustomNoUpgrade is configured
- OCPBUGS-36759 - [UI] RWOP accessMode is not available on OpenShift console UI
- OCPBUGS-36764 - Block all z rollbacks again
- OCPBUGS-36775 - RHEL worker nodes no longer work due to missing MGLRU
- OCPBUGS-36777 - [CAPI install] envtest.kubeconfig is not deleted when destroying cluster
- OCPBUGS-36841 - [release-4.16] Operand details page shows incorrect API version
- OCPBUGS-36854 - Cherry-pick Prometheus remote-write bug fix up to 4.16
- OCPBUGS-36862 - 4.16 "Bad" reconciliation loops can cause unbounded dockercfg secret creation
- OCPBUGS-36890 - [CAPI Azure] capi processes are still running when installer failed to start cluster-api-provider-azureaso and exited
- OCPBUGS-36907 - better handling of deprecated parameter in cluster-monitoring-config
- OCPBUGS-36959 - ART requests updates to 4.16 image ptp-operator-must-gather-container

- OCPBUGS-37063 - [release-4.16] 'View all steps in documentation' link should be hidden for ROSA and OSD
- OCPBUGS-37072 - ART requests updates to 4.16 image ose-ptp-operator-container
- OCPBUGS-37241 - hypershift ignition server uses RHEL major version mismatched MCO binaries

CVEs

- CVE-2023-27522
- CVE-2023-48795
- CVE-2024-3727
- CVE-2024-5564
- CVE-2024-6104
- CVE-2024-6409
- CVE-2024-24788
- CVE-2024-24790
- CVE-2024-32487

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 and Opt-Out Rights