RHSA-2024:4156 - Security Advisory

Issued: 2024-07-03 Updated: 2024-07-03

Synopsis

Important: OpenShift Container Platform 4.16.1 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.16.1 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 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 4.16.1. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2024:4159

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):

- openshift/telemeter: iss check during JWT authentication can be bypassed

(CVE-2024-5037)

- helm: Missing YAML Content Leads To Panic (CVE-2024-26147)

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:c17d4489c1b283ee71c76dda559e66a546e16b208a57eb156ef38fb30098903a

(For s390x architecture)
The image digest is
sha256:b24f28935370ec725cc326cf2cea24b0996b57552cfd009bed00314e4d8f0d2a

(For ppc64le architecture)
The image digest is
sha256:ac0d87fc7c9a78d68d0111fc061d5599e6d46a90fea4f8360f70ab1f0cd36d82

(For aarch64 architecture)
The image digest is
sha256:819d7a86c4280cde30d59b44d4b6abafb5e12f65c4b2d2ee604581547ba2e4b1

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 - 2265440 - CVE-2024-26147 helm: Missing YAML Content Leads To Panic
- BZ - 2272339 - CVE-2024-5037 openshift/telemeter: iss check during JWT authentication can be bypassed
- OCPBUGS-19007 - OCB builds fail when several MCPs are building at the same time
- OCPBUGS-25164 - 4.15 server does not have PodMetrics/NodeMetrics
- OCPBUGS-27190 - It should deny creating an ImageDigestMirrorSet with conflicting mirrorSourcePolicy
- OCPBUGS-30978 - crio memory usage increases with port-forward
- OCPBUGS-31275 - Some GCP install-config examples don't match with specs
- OCPBUGS-33864 - [console-plugin] Fix OCPBUGS-33587 and OCPBUGS-31082
- OCPBUGS-34214 - multus-admission-controller stuck in CrashLoopBackOff when egress IPs are created at scale [4.16]
- OCPBUGS-34261 - MachineOSConfig CurrentImagePullSecret field is not being used during image rollout
- OCPBUGS-34717 - The s2i build strategy is not assumed for Serverless Functions
- OCPBUGS-34837 - [backport 4.16] Ingress Operator E2E test failing with prometheus service account not found
- OCPBUGS-34968 - Deprecate PF4 and ReactRouter5 in SDK docs
- OCPBUGS-35023 - SIGSEGV installer runtime in Azure when validating subnet
- OCPBUGS-35049 - [capi aws] don't use S3 stub ignition for masters

- OCPBUGS-35056 - AWS - CPO can use incorrect CIDR range on the default worker security group
- OCPBUGS-35281 - Display of "Auth Token GCP" filter in OperatorHub should be conditioned
- OCPBUGS-35373 - InstallPlan fails with "updated validation is too restrictive" when multiple CRD versions are served
- OCPBUGS-35435 - vSphere UPI install fails during CAPI manifest creation
- OCPBUGS-35446 - vsphere-problem-detector - checkDataStoreWithURL fails both in newly installed and freshly upgraded 4.14 clusters
- OCPBUGS-35471 - Installer is ensuring userTags on subnets in BYO VPC deployments on AWS
- OCPBUGS-35472 - Helm dependency update to 3.14.4
- OCPBUGS-35476 - Race condition in CPMS presubmits can cause not found error
- OCPBUGS-35486 - IPv6 ingress VIP not configured in keepalived on vSphere Dual-stack
- OCPBUGS-35493 - [gcp] with N2D instance type, unexpectedly got error "Confidential Instance Config is only supported for compatible cpu platforms"
- OCPBUGS-35500 - update 4.16 CEO dev cert docs
- OCPBUGS-35515 - Feature parity with BYO Public IPv4 terraform in CAPA
- OCPBUGS-35527 - GHSA-6wvf-f2vw-3425: ose-installer-container: containers/image allows unexpected authenticated registry accesses
- OCPBUGS-35529 - Reusing installer state causes HostedZoneAlreadyExists failure
- OCPBUGS-35531 - [GCP CAPI install] the optional "kmsKeyServiceAccount" is demanded for controlPlane unexpectedly
- OCPBUGS-35557 - Migrate HyperShift KAS to none endpoint reconciler type
- OCPBUGS-35570 - aws bootstrap destroy due to awscluster modified
- OCPBUGS-35748 - [4.16] CoreOS node stuck with message "A start job is running for CoreOS Trigger Multipath"
- OCPBUGS-35755 - Fix etcd profiles e2e test to check returned status for updated value
- OCPBUGS-35838 - Remove KMS V1 provider support for IBM Cloud
- OCPBUGS-35873 - leap-seconds.list file included as part of linuxptp-daemon container expired on June 28, 2024
- OCPBUGS-35973 - After upgrading to 4.13 from 4.12 one of the worker node went into emergency mode.

CVEs

- CVE-2021-47400
- CVE-2023-28450
- CVE-2023-29483
- CVE-2023-34966
- CVE-2023-45289
- CVE-2023-45290

- CVE-2023-52425
- CVE-2023-52626
- CVE-2023-52667
- CVE-2024-2398
- CVE-2024-3727
- CVE-2024-5037
- CVE-2024-24783
- CVE-2024-24784
- CVE-2024-24785
- CVE-2024-24786
- CVE-2024-26147
- CVE-2024-26801
- CVE-2024-26974
- CVE-2024-27393
- CVE-2024-27397
- CVE-2024-27403
- CVE-2024-28176
- CVE-2024-28757
- CVE-2024-35870
- CVE-2024-35958
- CVE-2024-35960
- CVE-2024-36957

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/.

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