RHSA-2024:7174 - Security Advisory

Issued: 2024-10-02 Updated: 2024-10-02

Synopsis

Important: OpenShift Container Platform 4.16.15 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.16.15 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 4.16.15. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHBA-2024:7177

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):

- openstack-ironic: Specially crafted image may allow authenticated users

to gain access to potentially sensitive data (CVE-2024-44082)

- golang: net/http: golang: mime/multipart: golang: net/textproto: memory

exhaustion in Request.ParseMultipartForm (CVE-2023-45290)

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

(CVE-2024-3727)

- 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
sha256:7a478e987f9f283f7a182080522d40768db50ad274caad8165a9b5e74ba38c43

(For s390x architecture)
The image digest is
sha256:6c84cd13d6cc90038d11cee892b9398e6e49e78fc4caef06b7e589debab7f198

(For ppc64le architecture)
The image digest is
sha256:e0ca664a081cc992abc2303d2cdafc08b0cb961d8c5f9fe2ff9e91bd41788809

(For aarch64 architecture)
The image digest is
sha256:436f1c88a1dd46dc3a2f46ca6139dc998f013a28e7714ad59258e5f7ab7556d3

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 - 2268017 - CVE-2023-45290 golang: net/http: golang: mime/multipart: golang: net/textproto: memory exhaustion in Request.ParseMultipartForm
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2292787 - CVE-2024-24790 golang: net/netip: Unexpected behavior from Is methods for IPv4-mapped IPv6 addresses
- BZ - 2309331 - CVE-2024-44082 openstack-ironic: Specially crafted image may allow authenticated users to gain access to potentially sensitive data
- OCPBUGS-38112 - [release-4.16] Directly mutating links in useMemo may not result in re-render
- OCPBUGS-38964 - IngressController subnet selection in AWS
- OCPBUGS-39394 - [release-4.16] gather nmstate custom resources

- OCPBUGS-41372 - OpenID IDP endpoint verification fails when hostname can only be resolved by data plane
- OCPBUGS-41611 - 4.16: Disable:Broken for [sig-builds][Feature:Builds][Slow] can use private repositories as build input build using an HTTP token should be able to clone source code via an HTTP token [apigroup:build.openshift.io]
- OCPBUGS-41717 - Kube-aggregator reaching stale apiservice endpoints
- OCPBUGS-41840 - Built-in join subnet "100.64.0.0/16" overlaps cluster subnet "100.64.0.0/15" even though internalJoinSubnet is configured
- OCPBUGS-41845 - Slow network causes metal IPI bootstrap to fail
- OCPBUGS-41885 - IPI vSphere disconnected installation fails to use template in 4.16
- OCPBUGS-41967 - user workload monitoring is trying to scrap RH operators which have been installed in openshift-operators namespace
- OCPBUGS-42061 - Failure to pull NTO image preventing startup of ocp-tuned-one-shot.service
- OCPBUGS-42067 - Speed up CMO e2e tests [4.16.z]
- OCPBUGS-42159 - High number of redundant kubeproxy rules present in OCP 4.15 with OpenshiftSDN
- OCPBUGS-42222 - NMstate operator unusable after 2 weeks of use due to failed certificate validation
- OCPBUGS-42286 - [IBMCloud] MonitorTests fail due to CSI Driver pods require ClusterRole SCC binding

CVEs

- CVE-2020-12762
- CVE-2021-29390
- CVE-2021-40153
- CVE-2021-41043
- CVE-2021-41072
- CVE-2021-43618
- CVE-2022-24963
- CVE-2022-40090
- CVE-2022-44638
- CVE-2022-48468
- CVE-2022-48554
- CVE-2022-48622
- CVE-2023-0666
- CVE-2023-0668
- CVE-2023-2855
- CVE-2023-2856
- CVE-2023-2858
- CVE-2023-2952

- CVE-2023-3618
- CVE-2023-4641
- CVE-2023-6004
- CVE-2023-6228
- CVE-2023-6918
- CVE-2023-7104
- CVE-2023-22745
- CVE-2023-23931
- CVE-2023-25193
- CVE-2023-29491
- CVE-2023-32573
- CVE-2023-33285
- CVE-2023-33460
- CVE-2023-34410
- CVE-2023-37369
- CVE-2023-38197
- CVE-2023-38469
- CVE-2023-38470
- CVE-2023-38471
- CVE-2023-38472
- CVE-2023-38473
- CVE-2023-40745
- CVE-2023-41175
- CVE-2023-43785
- CVE-2023-43786
- CVE-2023-43787
- CVE-2023-43788
- CVE-2023-43789
- CVE-2023-45290
- CVE-2023-46316
- CVE-2023-47038
- CVE-2024-1488
- CVE-2024-1737
- CVE-2024-1975
- CVE-2024-2398
- CVE-2024-3651
- CVE-2024-3652
- CVE-2024-3727
- CVE-2024-4076
- CVE-2024-5564

- CVE-2024-6119
- CVE-2024-6345
- CVE-2024-6409
- CVE-2024-6923
- CVE-2024-7383
- CVE-2024-22365
- CVE-2024-24790
- CVE-2024-24806
- CVE-2024-25062
- CVE-2024-25629
- CVE-2024-28182
- CVE-2024-28834
- CVE-2024-28835
- CVE-2024-32002
- CVE-2024-32004
- CVE-2024-32020
- CVE-2024-32021
- CVE-2024-32465
- CVE-2024-32487
- CVE-2024-34397
- CVE-2024-37370
- CVE-2024-37371
- CVE-2024-37891
- CVE-2024-38428
- CVE-2024-38476
- CVE-2024-39331
- CVE-2024-42353
- CVE-2024-44082
- CVE-2024-45490
- CVE-2024-45491
- CVE-2024-45492
- CVE-2024-45769
- CVE-2024-45770

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