RHSA-2024:8425 - Security Advisory

Issued: 2024-10-31 Updated: 2024-10-31

Synopsis

Important: OpenShift Container Platform 4.15.37 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.15.37 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 4.15.37. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2024:8428

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):

- go-git: Maliciously crafted Git server replies can lead to path traversal

and RCE on go-git clients (CVE-2023-49569)

- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames

causes DoS (CVE-2023-45288)

- encoding/gob: golang: Calling Decoder.Decode on a message which contains

deeply nested structures can cause a panic due to stack exhaustion
(CVE-2024-34156)

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

(CVE-2024-3727)

- net/http: Denial of service due to improper 100-continue handling in

net/http (CVE-2024-24791)

- cloudevents/sdk-go: usage of WithRoundTripper to create a Client leaks

credentials (CVE-2024-28110)

- jose-go: improper handling of highly compressed data (CVE-2024-28180)
- go/parser: golang: Calling any of the Parse functions containing deeply

nested literals can cause a panic/stack exhaustion (CVE-2024-34155)

- go/build/constraint: golang: Calling Parse on a "// +build" build tag

line with deeply nested expressions can cause a panic due to stack
exhaustion (CVE-2024-34158)

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:da7da5023f153df1417ead29ed0a6e0998c3016a4173ca1956cf05da918b6ccb

(For s390x architecture)
The image digest is
sha256:e128f95fd4c5edb0fd632f21a9536a0d83ee160abc3c207209e63811db61f1b5

(For ppc64le architecture)
The image digest is
sha256:b28ec45481140342793dec40424d8c775f6cceabc626b1591f62da8eea206648

(For aarch64 architecture)
The image digest is
sha256:4a2cb3e13cdf9d41c5514355c8596e61883b4870b89876f906d5ec44653138be

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 - 2258143 - CVE-2023-49569 go-git: Maliciously crafted Git server replies can lead to path traversal and RCE on go-git clients
- BZ - 2268273 - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- BZ - 2268372 - CVE-2024-28110 cloudevents/sdk-go: usage of WithRoundTripper to create a Client leaks credentials
- BZ - 2268854 - CVE-2024-28180 jose-go: improper handling of highly compressed data
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2295310 - CVE-2024-24791 net/http: Denial of service due to improper 100-continue handling in net/http
- BZ - 2310527 - CVE-2024-34155 go/parser: golang: Calling any of the Parse functions containing deeply nested literals can cause a panic/stack exhaustion
- BZ - 2310528 - CVE-2024-34156 encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion
- BZ - 2310529 - CVE-2024-34158 go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion
- OCPBUGS-19254 - Update 4.15 openshift-enterprise-keepalived-ipfailover image to be consistent with ART
- OCPBUGS-39018 - Ironic inspection fails due to utf-8 decoding issue on Disk serial
- OCPBUGS-41838 - Post SDN to OVN live migration shows intermittent service connectivity failures for OSD on GCP cluster
- OCPBUGS-42335 - Slow network causes metal IPI bootstrap to fail
- OCPBUGS-42470 - List of default Camel K event sources disappears when adding a custom event source
- OCPBUGS-42471 - Need to allow blank for Project/namespace when setting SA Subject in 'Project access tab'
- OCPBUGS-42480 - Upgrade to 4.16 is blocked because root certificate has weak SHA1 signature algorithm
- OCPBUGS-42611 - Topology screen crashes when completed pod is selected
- OCPBUGS-42648 - Switch to use annotations as labels from PipelineRuns created through Pipelines as Code is deprecated

- OCPBUGS-42726 - oc adm prune deployments` does not work and giving panic when using --replica-set option
- OCPBUGS-42780 - Nodes to Node and subsequently pod to pod communication are repeatedly degrading despite multiple OVN DB rebuilds to fix the issue
- OCPBUGS-42881 - ROSA HCP Nodepool versions unexpectedly do not match Node versions
- OCPBUGS-42934 - Errors when the image registry is configured to use a custom Azure storage account located in a different resource group blocked the upgrade
- OCPBUGS-42992 - Hypershift is managing kubeconfigs for DNS and Ingress operators
- OCPBUGS-43057 - gather_network_logs_basics script when node is in the NotReady [backport 4.15]
- OCPBUGS-43468 - HCP unable to pull images from registries only accessible from worker nodes
- OCPBUGS-43626 - Load Red Hat keys in FIPS mode with Go 1.22
- OCPBUGS-43635 - OAuthServer service with Route type does not work with a custom hostname
- OCPBUGS-37704 - No ability to debug node-ip detection logic

CVEs

- CVE-2022-24805
- CVE-2022-24806
- CVE-2022-24807
- CVE-2022-24808
- CVE-2022-24809
- CVE-2022-24810
- CVE-2023-45288
- CVE-2023-49569
- CVE-2024-3727
- CVE-2024-5535
- CVE-2024-24791
- CVE-2024-28110
- CVE-2024-28180
- CVE-2024-34155
- CVE-2024-34156
- CVE-2024-34158
- CVE-2024-42353
- CVE-2024-44082

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/.