RHSA-2024:2047 - Security Advisory

Issued: 2024-05-02 Updated: 2024-05-02

Synopsis

Important: OpenShift Container Platform 4.13.41 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.13.41 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 4.13.

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

https://access.redhat.com/errata/RHSA-2024:2049

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/4.13/release_notes/ocp-4-13-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)

- go-git: Maliciously crafted Git server replies can cause DoS on go-git

clients (CVE-2023-49568)

- cluster-monitoring-operator: credentials leak (CVE-2024-1139)
- kubevirt-csi: PersistentVolume allows access to HCP's root node

(CVE-2024-1725)

- osin: manipulation of the argument secret leads to observable timing

discrepancy (CVE-2021-4294)

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 4.13 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/4.13/updating/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.13 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/4.13/release_notes/ocp-4-13-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:dbb8aa0cf53dc5ac663514e259ad2768d8c82fd1fe7181a4cfb484e3ffdbd3ba

(For s390x architecture)
The image digest is
sha256:421f1d408713576cd597aeabdeefb2cad6c6d4c1f40e0a88e9026911fb69aaaf

(For ppc64le architecture)
The image digest is
sha256:00283cbb7dceb54be3bea4f7d2b7877eac7dadcd952f0e4b0c3d95cf761f03bb

(For aarch64 architecture)
The image digest is
sha256:b6395664a18f7fe6ae8faf57a6be0490ffffa12b71dfa42e9515f91baa407a6f

All OpenShift Container Platform 4.13 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/4.13/updating/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.13 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.13 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 8 aarch64

Fixes

- BZ - 2156871 - CVE-2021-4294 osin: manipulation of the argument secret leads to observable timing discrepancy
- BZ - 2258143 - CVE-2023-49569 go-git: Maliciously crafted Git server replies can lead to path traversal and RCE on go-git clients
- BZ - 2258165 - CVE-2023-49568 go-git: Maliciously crafted Git server replies can cause DoS on go-git clients
- BZ - 2262158 - CVE-2024-1139 cluster-monitoring-operator: credentials leak
- BZ - 2265398 - CVE-2024-1725 kubevirt-csi: PersistentVolume allows access to HCP's root node
- OCPBUGS-22979 - [IBMCloud] Add IPI support for new region eu-es (Madrid)

- OCPBUGS-25922 - PromQL queries of the ""API Performance" dasboard can overload Thanos queriers
- OCPBUGS-28784 - ART requests updates to 4.13 image openshift-enterprise-console-operator-container
- OCPBUGS-31077 - Pipeline Name gets changed to "new-pipeline" on the Edit Pipeline YAML/Builder
- OCPBUGS-31505 - Bump to kubernetes 1.26.15
- OCPBUGS-31595 - [release-4.13] certificate signed by unknown authority while uninstalling operators from console.
- OCPBUGS-31702 - Autoscaler should scale from zero when taints do not have a "value" field
- OCPBUGS-31936 - tuned: tuned breaks dynamic IRQ affinity
- OCPBUGS-32143 - PTP consumer deployed with sidecar cannot get PTP events on getCurrentState call
- OCPBUGS-32334 - [csi-snapshot-controller-operator] does not create suitable role and roleBinding for csi-snapshot-webhook
- OCPBUGS-32359 - multi-arch libvirt jobs need yq-v4

CVEs

- CVE-2021-4294
- CVE-2021-26341
- CVE-2021-47099
- CVE-2022-1184
- CVE-2022-1852
- CVE-2022-3640
- CVE-2022-42895
- CVE-2022-48624
- CVE-2023-4408
- CVE-2023-5517
- CVE-2023-5679
- CVE-2023-6240
- CVE-2023-6516
- CVE-2023-49568
- CVE-2023-49569
- CVE-2023-50387
- CVE-2023-50868
- CVE-2024-1139
- CVE-2024-1488
- CVE-2024-1725
- CVE-2024-26582
- CVE-2024-26584
- CVE-2024-26586

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 Summit
