RHSA-2024:4329 - Security Advisory

Issued: 2024-07-11 Updated: 2024-07-11

Overview

Updated Images

Synopsis

Important: OpenShift Container Platform 4.14.32 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.14.32 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 4.14.

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

https://access.redhat.com/errata/RHBA-2024:4332

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/4.14/release_notes/ocp-4-14-release-notes.html

Security Fix(es):

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

(CVE-2024-5037)

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

(CVE-2023-48795)

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 4.14 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/4.14/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.14 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/4.14/release_notes/ocp-4-14-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
sha256:912d7c15e1d82ffc4aa1fc34d2b64c4c7b6670ecd11314c14ca2d6ffdcea22a3

(For s390x architecture)
The image digest is
sha256:c32644f572297e736d768d7bc3046e1e0bd1f5f210cff02f12e64bdfb3710ff7

(For ppc64le architecture)
The image digest is
sha256:9d2a77eb45f1c1785296d755de2c74e032891358818205ecaf185f39e64d3312

(For aarch64 architecture)
The image digest is
sha256:534f13d4930731691f09aec733ec80a6810aea908224d0384ac181e6c3a81144

All OpenShift Container Platform 4.14 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/4.14/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64

Fixes

- BZ - 2254210 - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- BZ - 2272339 - CVE-2024-5037 openshift/telemeter: iss check during JWT authentication can be bypassed
- OCPBUGS-30259 - Power VS: PlatformCredsCheck relies on endpoint that has been removed.
- OCPBUGS-32472 - cpuset changes after kubelet service restarts
- OCPBUGS-33942 - OpenShift vSphere Connection Configuration Does Not Appropriately Insert Escaped Strings
- OCPBUGS-33964 - Vague warning of VolumeResizeFailed on successful cephfs PVC expansion
- OCPBUGS-34885 - [OVN-IPSEC] During upgrade from 4.13 to 4.14 ovn-ipsec will stay in error state until all OVN stack is migrate
- OCPBUGS-35012 - Tuned devices_udev_regex=^INTERFACE=(?!!usb0) double exclamation mark

- OCPBUGS-35183 - [4.14] The secrets-store-csi-driver with AWS provider integration does not work in HyperShift hosted cluster
- OCPBUGS-35290 - Hosted Cluster etcd automatic defragmentation is not enabled by default
- OCPBUGS-35365 - router deployment fails on y-stream upgrade 4.13->4.14
- OCPBUGS-35401 - HCP: hypershift-operator on disconnected clusters ignores RegistryOverrides inspecting for nodepool release image(setting hypershift.openshift.io/control-plane-operator-image is a workaround)
- OCPBUGS-35475 - oc newapp unit tests are failing due to removed images
- OCPBUGS-35482 - HCP: imagesStreams on hosted-clusters pointing to image on private registries are failing due to tls verification although the registry is correctly trusted
- OCPBUGS-35520 - Race condition in CPMS presubmits can cause not found error
- OCPBUGS-35549 - Registry overrides are being propagated to some data plane components
- OCPBUGS-35553 - Bump to kubernetes 1.27.15
- OCPBUGS-35723 - Upgrade EventListener apiVersion to v1beta1
- OCPBUGS-35750 - [4.14] CoreOS node stuck with message "A start job is running for CoreOS Trigger Multipath"
- OCPBUGS-35826 - GHSA-6wvf-f2vw-3425: ose-installer-container: containers/image allows unexpected authenticated registry accesses
- OCPBUGS-35827 - vsphere: when esxi host is offline no version is present
- OCPBUGS-35877 - leap-seconds.list file included as part of linuxptp-daemon container expired on June 28, 2024
- OCPBUGS-35889 - GNSS EVENT state is not following O-Ran spec defined values
- OCPBUGS-35913 - vsphere-problem-detector - checkDataStoreWithURL fails both in newly installed and freshly upgraded 4.14 clusters
- OCPBUGS-35957 - [release-4.14] cluster-capi-operator: Fix gcp providers-list.yaml branch
- OCPBUGS-35989 - After upgrading to 4.13 from 4.12 one of the worker node went into emergency mode.
- OCPBUGS-36356 - kubelet does not start after reboot due to dependency issue
- OCPBUGS-36369 - checksum mismatch in go.mod cluster-api-operator@v0.2.0
- OCPBUGS-36416 - "alertmanager-trusted-ca-bundle configmap not injected in alertmanager-user-workload pods
- OCPBUGS-36464 - prometheus bound service token causing issues with version skew between mgmt and cluster-under-test

CVEs

- CVE-2020-12762
- CVE-2020-15778
- CVE-2020-26555
- CVE-2020-28241

- CVE-2021-46848
- CVE-2021-46909
- CVE-2021-46972
- CVE-2021-47069
- CVE-2021-47073
- CVE-2021-47236
- CVE-2021-47310
- CVE-2021-47311
- CVE-2021-47353
- CVE-2021-47356
- CVE-2021-47456
- CVE-2021-47495
- CVE-2022-4645
- CVE-2022-25255
- CVE-2022-27404
- CVE-2022-27405
- CVE-2022-27406
- CVE-2022-36227
- CVE-2022-40023
- CVE-2022-41862
- CVE-2022-47629
- CVE-2022-48337
- CVE-2022-48339
- CVE-2022-48624
- CVE-2023-0666
- CVE-2023-2856
- CVE-2023-2858
- CVE-2023-2952
- CVE-2023-2953
- CVE-2023-3446
- CVE-2023-3817
- CVE-2023-4016
- CVE-2023-4408
- CVE-2023-5090
- CVE-2023-5678
- CVE-2023-6004
- CVE-2023-6597
- CVE-2023-6918
- CVE-2023-7104
- CVE-2023-28450

- CVE-2023-32681
- CVE-2023-43785
- CVE-2023-43786
- CVE-2023-43787
- CVE-2023-43788
- CVE-2023-43789
- CVE-2023-45288
- CVE-2023-45289
- CVE-2023-45290
- CVE-2023-46316
- CVE-2023-48795
- CVE-2023-50387
- CVE-2023-50868
- CVE-2023-52464
- CVE-2023-52560
- CVE-2023-52615
- CVE-2023-52626
- CVE-2023-52667
- CVE-2023-52669
- CVE-2023-52675
- CVE-2023-52686
- CVE-2023-52700
- CVE-2023-52703
- CVE-2023-52781
- CVE-2023-52813
- CVE-2023-52835
- CVE-2023-52877
- CVE-2023-52878
- CVE-2023-52881
- CVE-2024-0450
- CVE-2024-1488
- CVE-2024-2398
- CVE-2024-3651
- CVE-2024-4467
- CVE-2024-5037
- CVE-2024-24783
- CVE-2024-25062
- CVE-2024-25629
- CVE-2024-26583
- CVE-2024-26584

- CVE-2024-26585
- CVE-2024-26656
- CVE-2024-26675
- CVE-2024-26735
- CVE-2024-26759
- CVE-2024-26801
- CVE-2024-26804
- CVE-2024-26826
- CVE-2024-26859
- CVE-2024-26906
- CVE-2024-26907
- CVE-2024-26974
- CVE-2024-26982
- CVE-2024-27397
- CVE-2024-27410
- CVE-2024-28182
- CVE-2024-28834
- CVE-2024-32002
- CVE-2024-32004
- CVE-2024-32020
- CVE-2024-32021
- CVE-2024-32465
- CVE-2024-32487
- CVE-2024-33599
- CVE-2024-33600
- CVE-2024-33601
- CVE-2024-33602
- CVE-2024-34064
- CVE-2024-35789
- CVE-2024-35835
- CVE-2024-35838
- CVE-2024-35845
- CVE-2024-35852
- CVE-2024-35853
- CVE-2024-35854
- CVE-2024-35855
- CVE-2024-35888
- CVE-2024-35890
- CVE-2024-35958
- CVE-2024-35959

- CVE-2024-35960
- CVE-2024-36004
- CVE-2024-36007

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/.