RHSA-2024:9620 - Security Advisory

Issued: 2024-11-20 Updated: 2024-11-20

Synopsis

Important: OpenShift Container Platform 4.14.41 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.14.41 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 4.14.

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

https://access.redhat.com/errata/RHSA-2024:9623

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-console: OAuth2 insufficient state parameter entropy

(CVE-2024-6508)

- dompurify: nesting-based mutation XSS vulnerability (CVE-2024-47875)
- dompurify: DOMPurify vulnerable to tampering by prototype pollution

(CVE-2024-48910)

- QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server

During Socket Closure (CVE-2024-7409)

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 as follows:

(For x86_64 architecture)
The image digest is
sha256:f4c6252655cea21b790ab6bd8d88da9a657d787a365cedf79bcab8371eb11290

(For s390x architecture)
The image digest is
sha256:b7a9b6bebff381cd86dd38747a43045fba0f2ff1903c87ac551d7cada723ebcb

(For ppc64le architecture)
The image digest is
sha256:6823347a606e8ea4e08708bbc8ca3fefa60f3b2659d86478885b6f7405baf14b

(For aarch64 architecture)
The image digest is
sha256:870cc14058a63d173f50f7a2f8d0140e48e6f283bc8521584f1e73002cc17d5f

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 - 2295777 - CVE-2024-6508 openshift-console: OAuth2 insufficient state parameter entropy
- BZ - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- BZ - 2318052 - CVE-2024-47875 dompurify: nesting-based mutation XSS vulnerability
- BZ - 2322949 - CVE-2024-48910 dompurify: DOMPurify vulnerable to tampering by prototype pollution
- OCPBUGS-42111 - Node sclaling failed due to misconfigurations in on-prem-resolv-prepender.service in RHOCP4
- OCPBUGS-43490 - Backport SDN migration API changes to 4.14
- OCPBUGS-43647 - [4.14] Cloud Credentials operator generating millions of messages per day in GCP clusters

- OCPBUGS-43980 - MCPs report wrong number of nodes when we move nodes from one custom MCP to another custom MCP
- OCPBUGS-43981 - Panic seen in CI job for MCC pod
- OCPBUGS-44002 - Continuous pull-secret updates / slow initialization on build01 (test platform infrastructure)
- OCPBUGS-44048 - Fix TestOperandProxyConfiguration and TestLeaderElection flakes on Image Registry Operator
- OCPBUGS-44095 - Backport SDN migration API changes for cluster config operator to 4.14
- OCPBUGS-44107 - network-edge DNS case failed: 'DNS should answer A and AAAA queries for a dual-stack service'
- OCPBUGS-44213 - Update admins to add CFE members
- OCPBUGS-44295 - Backwards compatibility for ENI tagging in AWS on HCP ROSA
- OCPBUGS-44304 - The setting of NTO cloud provider doesn't work
- OCPBUGS-44360 - [4.14] vSphere controller for surfacing CNS issue pre-upgrade
- OCPBUGS-44379 - OpenShift 4.14.40 downgrades libreswan to an older version with CVE exposure

CVEs

- CVE-2019-12900
- CVE-2022-48773
- CVE-2022-48936
- CVE-2023-52492
- CVE-2023-52522
- CVE-2024-3596
- CVE-2024-3652
- CVE-2024-6508
- CVE-2024-7006
- CVE-2024-7409
- CVE-2024-24857
- CVE-2024-26640
- CVE-2024-26656
- CVE-2024-26772
- CVE-2024-26851
- CVE-2024-26870
- CVE-2024-26906
- CVE-2024-26924
- CVE-2024-26976
- CVE-2024-27017
- CVE-2024-27062
- CVE-2024-31076

- CVE-2024-35839
- CVE-2024-35898
- CVE-2024-35939
- CVE-2024-38540
- CVE-2024-38541
- CVE-2024-38586
- CVE-2024-38608
- CVE-2024-39503
- CVE-2024-40924
- CVE-2024-40931
- CVE-2024-40961
- CVE-2024-40983
- CVE-2024-40984
- CVE-2024-41009
- CVE-2024-41039
- CVE-2024-41042
- CVE-2024-41066
- CVE-2024-41092
- CVE-2024-41093
- CVE-2024-42070
- CVE-2024-42079
- CVE-2024-42244
- CVE-2024-42271
- CVE-2024-42284
- CVE-2024-42292
- CVE-2024-42301
- CVE-2024-43854
- CVE-2024-43880
- CVE-2024-43889
- CVE-2024-43892
- CVE-2024-44935
- CVE-2024-44989
- CVE-2024-44990
- CVE-2024-45018
- CVE-2024-46826
- CVE-2024-46858
- CVE-2024-47668
- CVE-2024-47875
- CVE-2024-48910
- CVE-2024-49768

- CVE-2024-49769
- CVE-2024-50602

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/.