RHSA-2025:2710 - Security Advisory

Issued: 2025-03-19 Updated: 2025-03-19

Synopsis

Important: OpenShift Container Platform 4.14.49 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.14.49 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 4.14.49. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2025:2712

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.redhat.com/en/documentation/openshift_container_platform/4.14/html/release_notes/

Security Fix(es):

- buildah: Buildah allows arbitrary directory mount (CVE-2024-9675)
- bind: bind9: Many records in the additional section cause CPU exhaustion

(CVE-2024-11187)

- podman: buildah: Container breakout by using --jobs=2 and a race

condition when building a malicious Containerfile (CVE-2024-11218)

- runc: file descriptor leak (CVE-2024-21626)
- golang.org/x/net/html: Non-linear parsing of case-insensitive content in

golang.org/x/net/html (CVE-2024-45338)

- kernel: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy

and Mbox devices (CVE-2024-53197)

- Podman: Buildah: CRI-O: symlink traversal vulnerability in the

containers/storage library can cause Denial of Service (DoS)
(CVE-2024-9676)

- kernel: HID: core: zero-initialize the report buffer (CVE-2024-50302)

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.redhat.com/en/documentation/openshift_container_platform/4.14/html-single/updating_clusters/index#updating-cluster-cli.

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.redhat.com/en/documentation/openshift_container_platform/4.14/html/release_notes/

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:aad28ca69006c0cea18fc7487ab220bc5b627168dd49f112183428cb6bb32b62

(For s390x architecture)
The image digest is
sha256:5cfdd7e18af6e04ea3e69ad513655ad1a3e2917addb59d64e3fd027f6744b693

(For ppc64le architecture)
The image digest is
sha256:b05ebaa64e24c93704a8879e0fc9561029433aa1face919c5a1283bac316723c

(For aarch64 architecture)
The image digest is
sha256:0650436dc25bbe30f2b037e49971c135e0787fc6e20826f6c30cf71ea5880a74

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.redhat.com/en/documentation/openshift_container_platform/4.14/html-single/updating_clusters/index#updating-cluster-cli.

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 - 2258725 - CVE-2024-21626 runc: file descriptor leak

- BZ - 2317458 - CVE-2024-9675 buildah: Buildah allows arbitrary directory mount
- BZ - 2317467 - CVE-2024-9676 Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS)
- BZ - 2326231 - CVE-2024-11218 podman: buildah: Container breakout by using --jobs=2 and a race condition when building a malicious Containerfile
- BZ - 2327169 - CVE-2024-50302 kernel: HID: core: zero-initialize the report buffer
- BZ - 2333122 - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- BZ - 2334412 - CVE-2024-53197 kernel: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy and Mbox devices
- BZ - 2342879 - CVE-2024-11187 bind: bind9: Many records in the additional section cause CPU exhaustion
- OCPBUGS-42971 - [release-4.14] Collect number of resources in etcd by must-gather
- OCPBUGS-46606 - Power VS: Available SysTypes should be decided by zone rather than region
- OCPBUGS-48084 - [4.14] Update must-gather owners (artificial PR for backports)
- OCPBUGS-49753 - ImagePullSecret getting duplicated when editing DeploymentConfig in Form View
- OCPBUGS-50477 - HPA/oc scale and DeploymenConfig is not working
- OCPBUGS-50631 - machine-config-daemon pod not picking up on label and mcp change to push out new rendered- config
- OCPBUGS-50662 - [release-4.14] Increase waitForFallbackDegradedConditionTimeout of test e2e-sno-disruptive
- OCPBUGS-51044 - [openshift-4.15] OWNERS update for build componet
- OCPBUGS-51045 - [release-4.14] failed to provision volume with StorageClass "thin-csi-default"
- OCPBUGS-51363 - 4.15: 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]

CVEs

- CVE-2022-49043
- CVE-2023-52922
- CVE-2024-9675
- CVE-2024-9676
- CVE-2024-11187
- CVE-2024-11218
- CVE-2024-21626
- CVE-2024-45338
- CVE-2024-50302
- CVE-2024-53197

- CVE-2024-56171
- CVE-2024-57807
- CVE-2024-57979
- CVE-2025-1244
- CVE-2025-24928

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/security/vulnerabilities/RHSB-2024-001

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.