



Red Hat Product Errata RHSA-2025:9765 - Security Advisory

RHSA-2025:9765 - Security Advisory

Issued: 2025-07-02 Updated: 2025-07-02

[Overview](#)[Updated Images](#)

Synopsis

Moderate: OpenShift Container Platform 4.16.43 bug fix and security update

Type/Severity

Security Advisory: Moderate

Topic

Red Hat OpenShift Container Platform release 4.16.43 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 4.16.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 4.16.43. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHSA-2025:9766> 

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/4.16/html/release_notes/ 

Security Fix(es):

- cri-o: Checkpoint restore can be triggered from different namespaces

(CVE-2024-8676)

- openshift-api: openshift-controller-manager/build: Build Process in


OpenShift Allows Overwriting of Node Pull Credentials (CVE-2024-45497)

- glibc: static setuid binary dlopen may incorrectly search LD_LIBRARY_PATH

(CVE-2025-4802)


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 4.16 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/4.16/html-single/updating_clusters/index#updating-cluster-cli. 

Solution

For OpenShift Container Platform 4.16 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/4.16/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

sha256:8597a1a05b1792619cf56734de97fabe5f7ff77a100060924b4f5740ec10f2e1

(For s390x architecture)

The image digest is

sha256:379c66f3c9f8aac11cdaa74614fd8d2b2c8a4626c3604f641d2ea7ee0d46be70

(For ppc64le architecture)

The image digest is


sha256:5a5897081b628d1330e7d23dd3bd3de71cb647152fb1ed3a4fc10a85c4265ce1

(For aarch64 architecture)

The image digest is

sha256:235fd4e1df9a004001768ee48ff44d102634c08b789cc37a329ad6a52f6ce13a



All OpenShift Container Platform 4.16 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/4.16/html-single/updating_clusters/index#updating-cluster-cli. 

Affected Products

- Red Hat OpenShift Container Platform 4.16 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 9 aarch64

Fixes

- [BZ - 2308673](#)  - CVE-2024-45497 openshift-api: openshift-controller-manager/build: Build Process in OpenShift Allows Overwriting of Node Pull Credentials
- [BZ - 2313842](#)  - CVE-2024-8676 cri-o: Checkpoint restore can be triggered from different namespaces

- [BZ-2367468](#) - CVE-2025-4802 glibc: static setuid binary dlopen may incorrectly search LD_LIBRARY_PATH
- [OCPBUGS-14749](#) - FeatureGate change not triggering NodePool update of kubelet.conf
- [OCPBUGS-48121](#) - Node pending to reboot due to error in syncing cache for *v1.EgressFirewall informer in OCP with 300-500 worker nodes
- [OCPBUGS-48283](#) - [4.16] NNCP cannot update DNS nameserver on OCP
- [OCPBUGS-49391](#) - [4.16] Routes with SHA1 CA certificate break HAProxy reloading
- [OCPBUGS-54457](#) - openshift-sdn: No response from openshift router / Ingress when client port is 22623 or 22624
- [OCPBUGS-55697](#) - Add validation to check that NamedCertificates and the Internal Certificate SAN does not have conflicting domains
- [OCPBUGS-56242](#) - [4.16z] ovnkube-controller container is crashing with a panic: runtime error:
- [OCPBUGS-56704](#) - aws/edge failing e2e test: [sig-network][Feature:tap] should create a pod with a tap interface
- [OCPBUGS-56812](#) - [release-4.16] ovnkube-node-* crashed when node deleted
- [OCPBUGS-56981](#) - ccoctl crashes with nil pointer exception when creating Azure managed identity role assignments that already exist
- [OCPBUGS-57096](#) - [release-4.16] `go mod tidy; go mod vendor` makes changes to staging
- [OCPBUGS-57203](#) - "[sig-node-tuning] NTO should SNO installation does not finish due to wait for non-existing machine-config" failures for periodic-ci-openshift-release-master-nightly-4.16/4.17-e2e-agent-single-node-ipv6-conformance
- [OCPBUGS-57270](#) - Debug pod logs are not accessible when debugging a node via OpenShift Console
- [OCPBUGS-57290](#) - [4.16] Kubelet metrics endpoints experiencing prolonged outages
- [OCPBUGS-57326](#) - unhandled error: TypeError: L.b.logoutOpenShift is not a function
- [OCPBUGS-57494](#) - Proxy variables are not passed to machine config daemon pods when upgrade strategy is set to inPlace
- [OCPBUGS-58028](#) - Sync stable branch for cluster-api-provider-openstack release-0.10 into release-4.16

CVEs

- [CVE-2023-40403](#)
- [CVE-2023-52623](#)
- [CVE-2023-52662](#)
- [CVE-2024-8676](#)
- [CVE-2024-26638](#)
- [CVE-2024-26669](#)
- [CVE-2024-26939](#)
- [CVE-2024-35838](#)

- [CVE-2024-35847](#)
- [CVE-2024-36917](#)
- [CVE-2024-41042](#)
- [CVE-2024-45497](#)
- [CVE-2024-56615](#)
- [CVE-2024-58099](#)
- [CVE-2025-4802](#)
- [CVE-2025-21764](#)
- [CVE-2025-22871](#)


References

- <https://access.redhat.com/security/updates/classification/#moderate>

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



The image shows the Red Hat logo (a red hat) and the text "Red Hat" in white on a dark background. To the right of the logo are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo is a navigation menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites", each with a downward-pointing chevron icon to its right.

 Partial system outage



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)