



# RHSA-2025:3297 - Security Advisory

Issued: 2025-04-02    Updated: 2025-04-03

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

## Synopsis

Important: OpenShift Container Platform 4.17.23 bug fix and security update

## Type/Severity

Security Advisory: Important

## Topic

Red Hat OpenShift Container Platform release 4.17.23 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 4.17.

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

<https://access.redhat.com/errata/RHBA-2025:3299> 

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/4.17/html/release\\_notes/](https://docs.redhat.com/en/documentation/openshift_container_platform/4.17/html/release_notes/) 

Security Fix(es):

- grub2: net: Out-of-bounds write in grub\_net\_search\_config\_file()

(CVE-2025-0624)


- libxml2: Stack-based buffer overflow in xmlSprintfElements of libxml2

(CVE-2025-24928)

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


(CVE-2024-8676)


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 4.17 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/4.17/html-single/updating\\_clusters/index#updating-cluster-cli](https://docs.redhat.com/en/documentation/openshift_container_platform/4.17/html-single/updating_clusters/index#updating-cluster-cli). 

## Solution

For OpenShift Container Platform 4.17 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/4.17/html/release\\_notes/](https://docs.redhat.com/en/documentation/openshift_container_platform/4.17/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

sha256:7e8b4557c0a15765440c543ab50cd591bb94f0745c20564e5f15d57bf5f76a82

(For s390x architecture)

The image digest is

sha256:dd3148c37d8b4122f500ae1bb92e29e34d1cc3bfa634d5c53a9f8528945abd2d

(For ppc64le architecture)


The image digest is

sha256:04bf2f5c15417eeb7de26d95de767b62ce263d5cc99400cbaa4d370c5007ab18

(For aarch64 architecture)

The image digest is





sha256:b491dcca8f5a2fe177f628f661a23086497440cf9b994638b199b9299335741b

All OpenShift Container Platform 4.17 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/4.17/html-single/updating\\_clusters/index#updating-cluster-cli](https://docs.redhat.com/en/documentation/openshift_container_platform/4.17/html-single/updating_clusters/index#updating-cluster-cli). 

## Affected Products

- Red Hat OpenShift Container Platform 4.17 for RHEL 9 x86\_64
- Red Hat OpenShift Container Platform 4.17 for RHEL 8 x86\_64
- Red Hat OpenShift Container Platform for Power 4.17 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.17 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 8 aarch64

## Fixes

- [BZ - 2313842](#)  - CVE-2024-8676 cri-o: Checkpoint restore can be triggered from different namespaces
- [BZ - 2346112](#)  - CVE-2025-0624 grub2: net: Out-of-bounds write in grub\_net\_search\_config\_file()
- [BZ - 2346421](#)  - CVE-2025-24928 libxml2: Stack-based buffer overflow in xmlSprintfElements of libxml2
- [OCPBUGS-48439](#)  - kubevirt hosted cluster with apiserver noderport using hostname ends without network policies

- [OCPBUGS-49816](#) - [4.17] Non-admin users cannot read or modify UserDefinedNetwork CRs
- [OCPBUGS-51117](#) - Openshift console overview shows "No alert found" when clicked on view details.
- [OCPBUGS-52961](#) - openshift-install is not removing agent base temp folder
- [OCPBUGS-53071](#) - fix missing Pod disruption reasons
- [OCPBUGS-53086](#) - [release-4.17] Update the monitoring topic used by the console team
- [OCPBUGS-53283](#) - The openshift-operator-lifecycle-manager and openshift-marketplace namespaces still use old pod-security.kubernetes.io/\*-version v1.24 and v1.25 respectively
- [OCPBUGS-53441](#) - oc describe machineconfignodes output has a typo in the message field

## CVEs

- [CVE-2024-8676](#)
- [CVE-2025-0624](#)
- [CVE-2025-24928](#)
- [CVE-2025-27144](#)

## References

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

---

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



Quick Links



Help



Site Info



Related Sites



 All systems operational



[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 and Opt-Out Rights](#)