

[Subscriptions](#) | [Downloads](#) | [Red Hat Catalog](#) | [Get Support](#)



Cookie Preferences and Opt-Out Rights

Your Choices About Cookies on this Site



Red Hat F
RHSA A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

5-10-22

Overview When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Synop

Importa

Type/

Security

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Topic

Red Hat OpenShift Container Platform release 4.19.17 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 4.19.

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

<https://access.redhat.com/errata/155269> [↗](#)

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/4.19/html/release_notes/
↗

Security Fix(es):

- libarchive: Double free at archive_read_format_rar_seek_data() in archive_read_support_format_rar.c (CVE-2025-5914)
- unbound: Unbound Cache poisoning (CVE-2025-5994)
- sqlite: Integer Truncation in SQLite (CVE-2025-6965)
- podman: Podman kube play command may overwrite host files (CVE-2025-9566)
- libxml: Heap use after free (UAF) leads to Denial of service (DoS) (CVE-2025-49794)
- libxml: Type confusion leads to Denial of service (DoS) (CVE-2025-49796)

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 4.19 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/4.19/html-single/updating_clusters/index#updating-cluster-cli. ↗

Solution

For OpenShift Container Platform 4.19 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/4.19/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 {x864_DIGEST}

(For s390x architecture)


The image digest is {s390x_DIGEST}

(For ppc64le architecture)

The image digest is {ppc64le_DIGEST}

(For aarch64 architecture)

The image digest is {aarch64_DIGEST}

All OpenShift Container Platform 4.19 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/4.19/html-single/updating_clusters/index#updating-cluster-cli. 

Affected Products



- Red Hat OpenShift Container Platform 4.19 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.19 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.19 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.19 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.19 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.19 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.19 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.19 for RHEL 8 aarch64

Fixes


- [BZ - 2370861 !\[\]\(69baca079ef3ab6f03d58fd7e9f950f1_img.jpg\)](#) - CVE-2025-5914 libarchive: Double free at archive_read_format_rar_seek_data() in archive_read_support_format_rar.c
- [BZ - 2372373 !\[\]\(2da321c3dc978a55192cb9c452297973_img.jpg\)](#) - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- [BZ - 2372385 !\[\]\(957138edf7d2615e14984f6bdb665b72_img.jpg\)](#) - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- [BZ - 2380149 !\[\]\(37ed9c3cda1f09fc6bf9b8799015713a_img.jpg\)](#) - CVE-2025-6965 sqlite: Integer Truncation in SQLite
- [BZ - 2380949 !\[\]\(769552e38296ac66de798213d838f215_img.jpg\)](#) - CVE-2025-5994 unbound: Unbound Cache poisoning
- [BZ - 2393152 !\[\]\(bcb4bf60dddaf217b42faa0aa7ad10ac_img.jpg\)](#) - CVE-2025-9566 podman: Podman kube play command may overwrite host files

CVEs






- [CVE-2025-5914 !\[\]\(a724a4a68298d6dff85fe378e838a60a_img.jpg\)](#)
- [CVE-2025-5994 !\[\]\(e45f0f4def98e1246d9487bb157beff5_img.jpg\)](#)
- [CVE-2025-6965 !\[\]\(88bfc90d98dd4d34739a3a724db7c68c_img.jpg\)](#)
- [CVE-2025-9566 !\[\]\(ccf2eae7cfca7109675c84141018761f_img.jpg\)](#)


- [CVE-2025-49794](#) 
- [CVE-2025-49796](#) 


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/>.


**Red Hat**

Quick Links 

Help 

Site Info 

Related Sites 

 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 and Opt-Out Rights](#)