



# About cookies on this site



Red Hat F

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.

## RHSA

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.

i-03-05

Overview

Updated P

## Synop

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

Importa

Type/:

**Accept Default**

**Do Not Sell or Share My Personal Information**

Security Advisory: Important

[Cookie Preferences](#) | [Privacy Statement](#)

**Red Hat Lightspeed patch analysis**

Identify and remediate systems affected by this advisory.

[View affected systems](#)

## Topic

Red Hat OpenShift Container Platform release 4.17.19 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 RPM packages for Red Hat OpenShift Container Platform 4.17.19. See the following advisory for the container images for this release:


<https://access.redhat.com/errata/RHSA-2025:1912> 

Security Fix(es):

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


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

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.openshift.com/container-platform/4.17/release\\_notes/ocp-4-17-release-notes.html](https://docs.openshift.com/container-platform/4.17/release_notes/ocp-4-17-release-notes.html) 

## 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.openshift.com/container-platform/4.17/release\\_notes/ocp-4-17-release-notes.html](https://docs.openshift.com/container-platform/4.17/release_notes/ocp-4-17-release-notes.html) 


## 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 - 2326231](#)  - CVE-2024-11218 podman: buildah: Container breakout by using --jobs=2 and a race condition when building a malicious Containerfile

## CVEs


- [CVE-2024-11218](#) 

## 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 Do Not Sell or Share My Personal Information](#)