

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



# Cookie Preferences and Opt-Out Rights

## Your Choices 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**

**Advis**

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.

Overview

**Synop**

Importan

**Type/**

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.

Security Advisory: Important

**Topic**

Red Hat OpenShift Container Platform release 4.17.38 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 4.17.38. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHBA-2025:13976>

5-08-27

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):

- libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr (CVE-2025-7425)
- git: Git arbitrary code execution (CVE-2025-48384)
- git: Git arbitrary file writes (CVE-2025-48385)
- libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2 (CVE-2025-6021)
- libxml2: Out-of-Bounds Read in libxml2 (CVE-2025-32414)
- libxml2: Out-of-bounds Read in xmlSchemaDCFillNodeTables (CVE-2025-32415)

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:fea49ae633643615f8707ecbe801b484181b87db0746d2d85592768dbddf43c9

(For s390x architecture)

The image digest is

sha256:d3e9032b799e87cc82121c9da006d375845134120205fa2aa2edca033abf97d3

(For ppc64le architecture)

The image digest is

sha256:6c6251666a8e89289819cdb9dd7269d1ab2d90fdb96c2b15b2e04908d15fd88

(For aarch64 architecture)

The image digest is

sha256:3b83546dc680f6e3975faf101471c4e29fdc76f406327665e22f63ff406246c0

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

## Fixes


- [BZ - 2358121](#) [↗](#) - CVE-2025-32414 libxml2: Out-of-Bounds Read in libxml2
- [BZ - 2360768](#) [↗](#) - CVE-2025-32415 libxml2: Out-of-bounds Read in xmlSchemaDCFillNodeTables
- [BZ - 2372406](#) [↗](#) - CVE-2025-6021 libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2
- [BZ - 2378806](#) [↗](#) - CVE-2025-48384 git: Git arbitrary code execution
- [BZ - 2378808](#) [↗](#) - CVE-2025-48385 git: Git arbitrary file writes
- [BZ - 2379274](#) [↗](#) - CVE-2025-7425 libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr
- [OCPBUGS-54599](#) [↗](#) - [4.17] Bootimage bump tracker

## CVEs



- [CVE-2025-6021](#) [↗](#)
- [CVE-2025-7425](#) [↗](#)
- [CVE-2025-32414](#) [↗](#)
- [CVE-2025-32415](#) [↗](#)

- [CVE-2025-48384](#) 
- [CVE-2025-48385](#) 


## 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 

---

 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](#)