RHSA-2025:1120 - Security Advisory

Issued: 2025-02-11 Updated: 2025-02-11

Synopsis

Important: OpenShift Container Platform 4.17.16 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.17.16 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 4.17.16. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2025:1122

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.openshift.com/container-platform/4.17/release_notes/ocp-4-17-release-notes.html

Security Fix(es):

- python: Path traversal on tempfile.TemporaryDirectory (CVE-2023-6597)
- rsync: Info Leak via Uninitialized Stack Contents (CVE-2024-12085)
- golang.org/x/net/html: Non-linear parsing of case-insensitive content in

golang.org/x/net/html (CVE-2024-45338)

- unbound: Unbounded name compression could lead to Denial of Service

(CVE-2024-8508)

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.openshift.com/container-platform/4.17/updating/updating_a_cluster/updating-cluster-cli.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

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:e0907823bc8989b02bb1bd55d5f08262dd0e4846173e792c14e7684fbd476c0d

(For s390x architecture)
The image digest is
sha256:0ceb174ca670cfa3202ce15e1a884478bd4474c6bf2cf74fac0a44681bfbb8f3

(For ppc64le architecture)
The image digest is
sha256:460da6202791b5d3ec0ddd71a577723ffc68e35cf728ebbef832ef0a3c42e7be

(For aarch64 architecture)
The image digest is
sha256:4b48c890a1229bdb587fb4865fbebbb9f466e7e4a9bae0fbc7ec85352c5d6041

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.openshift.com/container-platform/4.17/updating/updating_a_cluster/updating-cluster-cli.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 - 2276518 - CVE-2023-6597 python: Path traversal on tempfile.TemporaryDirectory
- BZ - 2316321 - CVE-2024-8508 unbound: Unbounded name compression could lead to Denial of Service
- BZ - 2330539 - CVE-2024-12085 rsync: Info Leak via Uninitialized Stack Contents
- BZ - 2333122 - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- OCPBUGS-41300 - [CAPI Azure] Gen2 image definition missed security features enabled when configuring securitytype in install-config
- OCPBUGS-41596 - There is no need to supply "User workload notifications" option on "User Preference" page for normal user.
- OCPBUGS-42763 - [AWS CAPI install] Failed to create C2S/SC2S cluster via Cluster API

- OCPBUGS-44927 - [release-4.17 backport] MCE 2.7 create HostedCluster failed due to multi-arch check
- OCPBUGS-45740 - Function Import: An error occurred Cannot read properties of undefined (reading 'filter')
- OCPBUGS-49399 - telco openshift-apiserver panic observed
- OCPBUGS-49685 - The cluster storage operator is in a degraded state because it is unable to find the UUID for the Windows node.
- OCPBUGS-49758 - Layout incorrect for Service weight on Create Route page
- OCPBUGS-39602 - OCP sample application don't create BuildConfig resource
- OCPBUGS-45268 - ca-bundle.crt is not injected in the global-ca configmaps from builds in HCP cluster
- OCPBUGS-46465 - Cannot access external network via https from the HCP openshift-apiserver component
- OCPBUGS-49701 - [4.17] Handle HFC for non-redfish HW
- OCPBUGS-49756 - metal3-ramdisk-logs busy loop burning a core away

CVEs

- CVE-2023-6597
- CVE-2024-8508
- CVE-2024-12085
- CVE-2024-45338

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/.

Quick Links

Help

Site Info

Related Sites

Loading

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie preferences