RHSA-2024:10518 - Security Advisory

Issued: 2024-12-03   Updated: 2024-12-03

Synopsis

Important: OpenShift Container Platform 4.17.7 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.17.7 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 4.17.7. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHBA-2024:10521

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):

- pam: Improper Hostname Interpretation in pam_access Leads to Access

Control Bypass (CVE-2024-10963)

- go-retryablehttp: url might write sensitive information to log file

(CVE-2024-6104)

- QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server

During Socket Closure (CVE-2024-7409)

- cross-spawn: regular expression denial of service (CVE-2024-21538)

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:e8680baf0b44dc55accfe08c4ad298d508d5a19a371bc4747c2f6a92225aa38f

(For s390x architecture)
The image digest is sha256:ac5f1baaef0447c5010ddb9ff416e481274d045ca1641f00fccef680265fa47d

(For ppc64le architecture)
The image digest is
sha256:ded679380070f96330a9902eeccc9ee8b13f7b4588b6d0e7bf7bb1385bb568ab

(For aarch64 architecture)
The image digest is
sha256:ca82f8a3d13fa2a43a920f8be072df56ea3c24312592dce189039e8800c329be

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 - 2294000 - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- BZ - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- BZ - 2324291 - CVE-2024-10963 pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass
- BZ - 2324550 - CVE-2024-21538 cross-spawn: regular expression denial of service
- OCPBUGS-42752 - HPA/oc scale and DeploymenConfig is not working
- OCPBUGS-43047 - fix slice init length
- OCPBUGS-43454 - ovnkube-control-plane pods crash when upgrading from 4.16 to 4.17 with localnet topology networks without subnets
- OCPBUGS-43795 - While upgrading the cluster from UI observed ` Warning alert:Admission Webhook Warning`
- OCPBUGS-43800 - Azure Session for Client Certificate Credential Should Set Options to Send Certificate Chain
- OCPBUGS-44183 - [release-4.17] Remove ClusterTask dependency in console from Pipelines 1.17
- OCPBUGS-44190 - Fix unexpected node not ready being ignored
- OCPBUGS-44611 - [AWS] Node SG - Inbound rule access from 0.0.0.0/0 for node port range 30000-32767
- OCPBUGS-44699 - [regression] Impossible to pass multiline parameters to templates
- OCPBUGS-44764 - add IBM Block Storage CSI driver support for RWX
- OCPBUGS-44830 - unit test jobs in oc fail due to removed image

CVEs

- CVE-2022-48804
- CVE-2023-52619
- CVE-2023-52635
- CVE-2023-52775
- CVE-2023-52811
- CVE-2024-5569
- CVE-2024-6104
- CVE-2024-7409
- CVE-2024-10963
- CVE-2024-21538
- CVE-2024-26601
- CVE-2024-26615
- CVE-2024-26686
- CVE-2024-26704
- CVE-2024-27399
- CVE-2024-36960
- CVE-2024-38384
- CVE-2024-38541
- CVE-2024-38555
- CVE-2024-39507
- CVE-2024-40997
- CVE-2024-41007
- CVE-2024-41008
- CVE-2024-41009
- CVE-2024-41031
- CVE-2024-41038
- CVE-2024-41056
- CVE-2024-41093
- CVE-2024-42154
- CVE-2024-42228
- CVE-2024-42237
- CVE-2024-42238
- CVE-2024-42240
- CVE-2024-42241
- CVE-2024-42243
- CVE-2024-42244
- CVE-2024-42271
- CVE-2024-44309
- CVE-2024-44989

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/.