RHSA-2025:3798 - Security Advisory

Issued: 2025-04-16 Updated: 2025-04-16

Synopsis

Important: OpenShift Container Platform 4.17.25 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.17.25 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 4.17.25. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHBA-2025:3800

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/

Security Fix(es):

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

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

- golang-jwt/jwt: jwt-go allows excessive memory allocation during header

parsing (CVE-2025-30204)

- libxml: use-after-free in xmlXIncludeAddNode (CVE-2022-49043)
- baremetal-operator/apis: Bare Metal Operator (BMO) can expose any secret

from other namespaces via BMCEventSubscription CRD (CVE-2025-29781)

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.

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/

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
sha256:61b5415f1395d5b1266621031ff0d57969f7d086d1da5847e60b6ef549d692f6

(For s390x architecture)
The image digest is
sha256:94fe0e427e0e735b002c85c548b614c3991832f011e6416c144121e32e9c95b7

(For ppc64le architecture)
The image digest is
sha256:992523048257d51a46a80fd2870a26629deb2e436c18edb8841d9be994d9c787

(For aarch64 architecture)
The image digest is
sha256:81c11a4fad75f06d136b0ce4f639321aa47776f3076f1b4dff4c766bd17d36b9

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.

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
- BZ - 2342118 - CVE-2022-49043 libxml: use-after-free in xmlXIncludeAddNode
- BZ - 2353041 - CVE-2025-29781 baremetal-operator/apis: Bare Metal Operator (BMO) can expose any secret from other namespaces via BMCEventSubscription CRD
- BZ - 2354195 - CVE-2025-30204 golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing
- OCPBUGS-47471 - [backport 4.17] Multus thin plugin's CmdDel waits for API server indefinitely

- OCPBUGS-52188 - Cluster upgrade stuck due to machine-config CO in degraded state
- OCPBUGS-53415 - SNYK: Medium severity vulnerability found in github.com/golang/glog
- OCPBUGS-54211 - Unable to see the Alerts in his developer webUI
- OCPBUGS-54325 - Autoscaler does not work after entering in failed status for a single machineautoscaler
- OCPBUGS-54343 - [4.17] SELinux container_logreader_t cannot watch /var/log symlinks
- OCPBUGS-54542 - [4.17] Add missing relatedObjects to CBO
- OCPBUGS-54631 - [4.17] Hotplug volumes doesn't auto-reattachment to the same Node (kubevirt VM) when restarting so quick pod never reaches Terminating
- OCPBUGS-54693 - Add delay in linuxptp-daemon to wait for socket to be ready

CVEs

- CVE-2022-49043
- CVE-2024-2236
- CVE-2024-5535
- CVE-2024-11218
- CVE-2024-44192
- CVE-2024-54467
- CVE-2024-54551
- CVE-2024-55549
- CVE-2025-24208
- CVE-2025-24209
- CVE-2025-24216
- CVE-2025-29781
- CVE-2025-30204
- CVE-2025-30427

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