RHSA-2025:15397 - Security Advisory

Issued: 2025-10-21 Updated: 2025-10-21

Overview

Synopsis

Important: OpenShift Container Platform 4.20.0 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.20.0 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 4.20.

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 4.20.0. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/149403

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/4.20/html/release_notes/

Security Fix(es):

- libarchive: Double free at archive_read_format_rar_seek_data() in

archive_read_support_format_rar.c (CVE-2025-5914)

- unbound: Unbound Cache poisoning (CVE-2025-5994)
- podman: podman missing TLS verification (CVE-2025-6032)
- sqlite: Integer Truncation in SQLite (CVE-2025-6965)
- libxml: Heap use after free (UAF) leads to Denial of service (DoS)

(CVE-2025-49794)

- libxml: Type confusion leads to Denial of service (DoS) (CVE-2025-49796)

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 4.20 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/4.20/html-single/updating_clusters/index#updating-cluster-cli.

Solution

For OpenShift Container Platform 4.20 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/4.20/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:d1dc76522d1e235b97675b28e977cb8c452f47d39c0eb519cde02114925f91d2

(For s390x architecture)
The image digest is
sha256:bb2b07ca992b8c976341c145ccdcefbd57e946a590efaa5e10d60fc5a2cbe503

(For ppc64le architecture)
The image digest is
sha256:678369ac0a189674b3d9f5779ee7042b39e625ee580579ec302d8899f8ddc613

(For aarch64 architecture)
The image digest is
sha256:791079aeb081a9193cec139ba4dccbafbfc9437b6e5e39d70225b0e6d2f51b34

All OpenShift Container Platform 4.20 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/4.20/html-single/updating_clusters/index#updating-cluster-cli.

Affected Products

- Red Hat OpenShift Container Platform 4.20 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.20 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.20 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.20 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.20 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.20 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.20 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.20 for RHEL 8 aarch64

Fixes

- BZ - 2370861 - CVE-2025-5914 libarchive: Double free at archive_read_format_rar_seek_data() in archive_read_support_format_rar.c
- BZ - 2372373 - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- BZ - 2372385 - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- BZ - 2372501 - CVE-2025-6032 podman: podman missing TLS verification
- BZ - 2380149 - CVE-2025-6965 sqlite: Integer Truncation in SQLite
- BZ - 2380949 - CVE-2025-5994 unbound: Unbound Cache poisoning
- OCPBUGS-55905 - [4.20] Bootimage bump tracker

- OCPBUGS-55906 - Enable RHCOS IBM Secure Execution installation on IBM Z17
- OCPBUGS-56277 - Fix crun-wasm extension in RHEL 9.6 based RHOS
- OCPBUGS-56645 - [4.20] Bootimage bump tracker
- OCPBUGS-58117 - [4.20] Bootimage bump tracker
- OCPBUGS-59201 - [4.20] Nodes born on 4.1/4.2 will not be able to upgrade to 4.19 due to composefs + grub2-probe incompatibility
- OCPBUGS-59630 - Add kubevirt s390x artifact
- OCPBUGS-60099 - Remove fips.so overlay in the initrd
- OCPBUGS-60664 - [4.19] bootimage needs a refresh for linux-firmware updates required for GNR-D hardware

CVEs

- CVE-2025-5914
- CVE-2025-5994
- CVE-2025-6032
- CVE-2025-6965
- CVE-2025-49794
- CVE-2025-49796

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/.