RHSA-2024:4151 - Security Advisory

Issued: 2024-07-02 Updated: 2024-07-02

Synopsis

Important: OpenShift Container Platform 4.15.20 security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.15.20 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 4.15.

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

https://access.redhat.com/errata/RHBA-2024:4154

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/4.15/release_notes/ocp-4-15-release-notes.html

Security Fix(es):

- openshift/telemeter: iss check during JWT authentication can be bypassed

(CVE-2024-5037)

- ssh: Prefix truncation attack on Binary Packet Protocol (BPP)

(CVE-2023-48795)

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 4.15 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/4.15/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.15 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/4.15/release_notes/ocp-4-15-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

(For x86_64 architecture)
The image digest is
sha256:478d9f5a1b496ebd69ecd0d7a7fc961f6318290ac9242ff65e1e2bdb88ff3097

(For s390x architecture)
The image digest is
sha256:0792d79ae4e5428851e387b00695934d90c2dfeadff5b05ac7979ebe83e1a127

(For ppc64le architecture)
The image digest is
sha256:83daa09f3de75c73d8167c4c40f22c28562e07d645682abbbaf9b4963c7ff614

(For aarch64 architecture)
The image digest is
sha256:739580c2175f81df210310042e4fd1395344990d96a39498e1df919df7bb97ee

All OpenShift Container Platform 4.15 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/4.15/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.15 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.15 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 8 aarch64

Fixes

- BZ - 2254210 - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- BZ - 2272339 - CVE-2024-5037 openshift/telemeter: iss check during JWT authentication can be bypassed
- OCPBUGS-32404 - [release-4.15] Creation of second hostedcluster in the same namespace fails with 'failed to set secret''s owner reference'
- OCPBUGS-32501 - Pipeline details page Metrics tab crashed due to no custom data
- OCPBUGS-33642 - PF5 Modal is not rendered correctly in Openshift Console Dynamic Plugin
- OCPBUGS-33885 - Automatic scaling not always working because NodeGroup.GetOptions() not being implemented
- OCPBUGS-34478 - UI inconsistency in topology when application grouping is collapsed
- OCPBUGS-34579 - HCP: imagesStreams on hosted-clusters pointing to image on private registries are failing due to tls verification although the registry is correctly trusted
- OCPBUGS-35305 - [release-4.15] OLM catalog pods do not recover from node failure

- OCPBUGS-35359 - [gcp][CORS-2420] deploying compact 3-nodes cluster on GCP, by setting mastersSchedulable as true and removing worker machineset YAMLs, got panic
- OCPBUGS-35543 - IPv6 ingress VIP not configured in keepalived on vSphere Dual-stack
- OCPBUGS-35714 - AWS - CPO can use incorrect CIDR range on the default worker security group
- OCPBUGS-35732 - vsphere-problem-detector - checkDataStoreWithURL fails both in newly installed and freshly upgraded 4.14 clusters
- OCPBUGS-35865 - [release4.15] Insights Operator to collect the 'prometheus' and 'alertmanager' instances
- OCPBUGS-35872 - leap-seconds.list file included as part of linuxptp-daemon container expired on June 28, 2024
- OCPBUGS-35894 - The third master is not joining to the cluster on an Agent Based Installations

CVEs

- CVE-2019-25162
- CVE-2020-12762
- CVE-2020-15778
- CVE-2020-28241
- CVE-2020-36777
- CVE-2021-46848
- CVE-2021-46934
- CVE-2021-47013
- CVE-2021-47055
- CVE-2021-47118
- CVE-2021-47153
- CVE-2021-47171
- CVE-2021-47185
- CVE-2021-47400
- CVE-2022-4645
- CVE-2022-25255
- CVE-2022-27404
- CVE-2022-27405
- CVE-2022-27406
- CVE-2022-36227
- CVE-2022-41862
- CVE-2022-47629
- CVE-2022-48337
- CVE-2022-48339
- CVE-2022-48624
- CVE-2022-48627

- CVE-2022-48669
- CVE-2023-0666
- CVE-2023-2856
- CVE-2023-2858
- CVE-2023-2952
- CVE-2023-3446
- CVE-2023-3817
- CVE-2023-4016
- CVE-2023-4408
- CVE-2023-5678
- CVE-2023-6004
- CVE-2023-6240
- CVE-2023-6597
- CVE-2023-6918
- CVE-2023-7008
- CVE-2023-7104
- CVE-2023-28450
- CVE-2023-32681
- CVE-2023-34966
- CVE-2023-43785
- CVE-2023-43786
- CVE-2023-43787
- CVE-2023-43788
- CVE-2023-43789
- CVE-2023-45288
- CVE-2023-45289
- CVE-2023-45290
- CVE-2023-46316
- CVE-2023-48795
- CVE-2023-50387
- CVE-2023-50868
- CVE-2023-52439
- CVE-2023-52445
- CVE-2023-52477
- CVE-2023-52513
- CVE-2023-52520
- CVE-2023-52528
- CVE-2023-52565
- CVE-2023-52578
- CVE-2023-52594

- CVE-2023-52595
- CVE-2023-52598
- CVE-2023-52606
- CVE-2023-52607
- CVE-2023-52610
- CVE-2024-0340
- CVE-2024-0450
- CVE-2024-2398
- CVE-2024-5037
- CVE-2024-22365
- CVE-2024-23307
- CVE-2024-24783
- CVE-2024-25062
- CVE-2024-25744
- CVE-2024-26458
- CVE-2024-26461
- CVE-2024-26593
- CVE-2024-26603
- CVE-2024-26610
- CVE-2024-26615
- CVE-2024-26642
- CVE-2024-26643
- CVE-2024-26659
- CVE-2024-26664
- CVE-2024-26693
- CVE-2024-26694
- CVE-2024-26743
- CVE-2024-26744
- CVE-2024-26779
- CVE-2024-26872
- CVE-2024-26892
- CVE-2024-26897
- CVE-2024-26901
- CVE-2024-26919
- CVE-2024-26933
- CVE-2024-26934
- CVE-2024-26964
- CVE-2024-26973
- CVE-2024-26993
- CVE-2024-27014

- CVE-2024-27048
- CVE-2024-27052
- CVE-2024-27056
- CVE-2024-27059
- CVE-2024-27393
- CVE-2024-27397
- CVE-2024-27403
- CVE-2024-28834
- CVE-2024-32002
- CVE-2024-32004
- CVE-2024-32020
- CVE-2024-32021
- CVE-2024-32465
- CVE-2024-33599
- CVE-2024-33600
- CVE-2024-33601
- CVE-2024-33602
- CVE-2024-35870
- CVE-2024-35958
- CVE-2024-35960
- CVE-2024-36957

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

All systems operational

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