RHSA-2024:4960 - Security Advisory

Issued: 2024-08-07 Updated: 2024-08-07

Synopsis

Important: OpenShift Container Platform 4.14.34 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.14.34 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 4.14.

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

https://access.redhat.com/errata/RHSA-2024:4963

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/4.14/release_notes/ocp-4-14-release-notes.html

Security Fix(es):

- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames

causes DoS (CVE-2023-45288)

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA

payloads (CVE-2024-1394)

- dnspython: denial of service in stub resolver (CVE-2023-29483)
- ssh: Prefix truncation attack on Binary Packet Protocol (BPP)

(CVE-2023-48795)

- containers/image: digest type does not guarantee valid type

(CVE-2024-3727)

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

(CVE-2024-6104)

- openssh: Possible remote code execution due to a race condition in signal

handling affecting Red Hat Enterprise Linux 9 (CVE-2024-6409)

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 4.14 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/4.14/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.14 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/4.14/release_notes/ocp-4-14-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:d703e6615b85a6f94fb3f3e490f2eb4514412bc018ecfe967f57f4221116a718

(For s390x architecture)
The image digest is
sha256:5974477b97dd1b519790c6eaf644c8a4a00fe4347eb18551a94754075ca690dd

(For ppc64le architecture)
The image digest is
sha256:43013ace5c68f0ba4dd2b648df54e1bbd8a4cd4ed301cd252d2b403c0ca9180f

(For aarch64 architecture)
The image digest is
sha256:1eb0e157f57bebcfa8feed480479e540e60d93c4f93c951870002dbacd42c639

All OpenShift Container Platform 4.14 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/4.14/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x

- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64

Fixes

- BZ - 2254210 - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- BZ - 2262921 - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads
- BZ - 2268273 - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- BZ - 2274520 - CVE-2023-29483 dnspython: denial of service in stub resolver
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2294000 - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- BZ - 2295085 - CVE-2024-6409 openssh: Possible remote code execution due to a race condition in signal handling affecting Red Hat Enterprise Linux 9
- OCPBUGS-33022 - Missing 'ping' executable file on s390x node in origin tests:[sig-network][Feature:EgressFirewall]
- OCPBUGS-33367 - [Jira:"NetworkEdge"] monitor test service-type-load-balancer-availability setup fails frequently in 4.14 & 4.15 PowerVS CI jobs
- OCPBUGS-36159 - AWS - CPO can use incorrect CIDR range on the default worker security group
- OCPBUGS-36380 - [release4.14] Insights Operator to collect the 'prometheus' and 'alertmanager' instances
- OCPBUGS-36397 - Kube-scheduler panics in OCP 4.14 when Pod has invalid Node selector
- OCPBUGS-36452 - [4.14] Can't install operator on 4.15 after uninstalling it on a prior version
- OCPBUGS-36467 - [Backport 4.14] OCP upgrade from 4.13 to 4.14 triggers the error "failed to update canary route openshift-ingress-canary/canary"
- OCPBUGS-36555 - [release-4.14] Allow configuring router default connect timeout on an ingress controller
- OCPBUGS-36565 - PrometheusOperatorRejectedResources should link its runbook
- OCPBUGS-36716 - Cloud credential operator logs two errors per second when awsSTSIAMRoleARN is empty
- OCPBUGS-36748 - 4.14 PowerVS CI jobs are failing with error-" yq-v4: not found"
- OCPBUGS-36800 - 4.14: Build Tests Reference EOL Ruby Image
- OCPBUGS-36915 - Node fails to join cluster as CSR contains wrong hostname in dualstack setup
- OCPBUGS-37068 - [4.14] Bootimage bump tracker
- OCPBUGS-37204 - PTP operator showing high cpu utilization with steady workload on OCP 4.15

- OCPBUGS-37242 - Very high ts2phc offsets reported in linuxptp log while metrics show ts2phc clock_state is locked and GM clock_state is FREERUN
- OCPBUGS-37276 - Update to azidentity v1.7.0 [4.14]
- OCPBUGS-37502 - [4.14] haproxy crashlooping fresh install Openshift 4.14.10
- OCPBUGS-37197 - [4.14] ovs-vswitchd is using isolated cpu pool instead of reserved pool

CVEs

- CVE-2023-29483
- CVE-2023-45288
- CVE-2023-45289
- CVE-2023-45290
- CVE-2023-48795
- CVE-2024-1394
- CVE-2024-3727
- CVE-2024-5564
- CVE-2024-6104
- CVE-2024-6409
- CVE-2024-24783
- CVE-2024-24784
- CVE-2024-24785
- CVE-2024-24786
- CVE-2024-24788
- CVE-2024-28176
- CVE-2024-32487
- CVE-2024-34064
- CVE-2024-37298
- CVE-2024-38474
- CVE-2024-38475
- CVE-2024-38477

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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage

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