RHSA-2024:6406 - Security Advisory

Issued: 2024-09-11 Updated: 2024-09-11

Synopsis

Important: OpenShift Container Platform 4.14.36 security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.14.36 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 4.14.36. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2024:6412

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)

- bind: bind9: BIND's database will be slow if a very large number of RRs

exist at the same nam (CVE-2024-1737)

- bind9: bind: SIG(0) can be used to exhaust CPU resources (CVE-2024-1975)
- bind: bind9: Assertion failure when serving both stale cache data and

authoritative zone content (CVE-2024-4076)

- opentelemetry: DoS vulnerability in otelhttp (CVE-2023-45142)
- opentelemetry-go-contrib: DoS vulnerability in otelgrpc due to unbound

cardinality metrics (CVE-2023-47108)

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

(CVE-2023-48795)

- coredns: CD bit response is cached and served later (CVE-2024-0874)
- go-retryablehttp: url might write sensitive information to log file

(CVE-2024-6104)

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
sha256:4bc4925e8028158e3f313aa83e59e181c94d88b4aa82a3b00202d6f354e8dfed

(For s390x architecture)
The image digest is
sha256:788a7a0fd2d808d1107d7ffc6731f799bdb8a41ac01ffab2afdbcb83b3390ffa

(For ppc64le architecture)
The image digest is
sha256:f5c4474b162b3be7f693c51572d21dc5b1c8e14861049f2c426f4cce0a6bb4d8

(For aarch64 architecture)
The image digest is
sha256:0bad0cf89c81b99f44e8db697ff63c8b1acf973dc57cf138eadfd7708844027e

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 - 2219234 - CVE-2024-0874 coredns: CD bit response is cached and served later
- BZ - 2245180 - CVE-2023-45142 opentelemetry: DoS vulnerability in otelhttp

- BZ - 2251198 - CVE-2023-47108 opentelemetry-go-contrib: DoS vulnerability in otelgrpc due to unbound cardinality metrics
- BZ - 2254210 - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- BZ - 2268273 - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- BZ - 2294000 - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- BZ - 2298893 - CVE-2024-1737 bind: bind9: BIND's database will be slow if a very large number of RRs exist at the same nam
- BZ - 2298901 - CVE-2024-1975 bind9: bind: SIG(0) can be used to exhaust CPU resources
- BZ - 2298904 - CVE-2024-4076 bind: bind9: Assertion failure when serving both stale cache data and authoritative zone content
- OCPBUGS-30414 - openshift/images repository lacks a CI job to run unit tests
- OCPBUGS-32258 - nodeip-configuration doesn't log to serial console
- OCPBUGS-32706 - multus-admission-controller stuck in CrashLoopBackOff when egress IPs are created at scale [4.14]
- OCPBUGS-33748 - PipelineRun details page break for pipeline with when expression using CEL expression
- OCPBUGS-35223 - Need a ptpOperatorConfig webhook to prevent users from creating a new event config (instead of using default)
- OCPBUGS-35846 - IPv6 ingress VIP not configured in keepalived on vSphere Dual-stack
- OCPBUGS-36161 - [release-4.14]Dynamic update of leap file path in linuxptp daemon
- OCPBUGS-36180 - [OCP 4.14] baremetal IPI without provisioning network failing on provisioning-interface.service
- OCPBUGS-36223 - [release-4.14]Dynamic update of leap file path in ptp operator
- OCPBUGS-37076 - Fix audit-logs container to respect SIGTERM
- OCPBUGS-37221 - Network node identity uses unescaped IPv6 addresses in the ValidatingWebhookConfiguration
- OCPBUGS-37673 - [release4.14] Ingress controller related certificates' validate dates gathering
- OCPBUGS-37728 - Backport owners file for network-metrics-daemon
- OCPBUGS-37754 - NTO operand reloads TuneD unnecessarily twice
- OCPBUGS-37823 - GCP cluster with CCO Passthrough mode failed to install due to CCO degraded
- OCPBUGS-37966 - T-GM : ts2phc process restart doesn't update PTP syncState when the process recovered
- OCPBUGS-38053 - Restarting baremetal nodes from RHOCP GUI is not working
- OCPBUGS-38371 - 4.12 -> 4.13 upgrade using IPI on Azure does not work
- OCPBUGS-38378 - snyk: google.golang.org/grpc/metadata [4.14]

- OCPBUGS-38544 - The Catalog Operator attempts to connect to deleted catalogSources
- OCPBUGS-38624 - Removing old weak ciphers from security profile for Hypershift hosted cluster
- OCPBUGS-38786 - nodeip-configuration.service is disabled to start during system startup on RHCOS on OCP cluster nodes on AWS
- OCPBUGS-38791 - discoverOpenIDURLs and checkOIDCPasswordGrantFlow fail if endpoints are private to the data plane
- OCPBUGS-38959 - Kubelet will not output logs after log file is rotated
- OCPBUGS-39160 - Centos8 is EOL Update to 9
- OCPBUGS-39176 - noProxy URL not available in Prometheus k8s CR after configuring remote-write
- OCPBUGS-39230 - HCP CCMs attempt direct internet access with proxied management cluster
- OCPBUGS-38263 - [4.14] While upgrading from 4.12.55 to 4.13.42, the network operator goes in a degraded state due to the ovnkube-master pods ending up in a crashloopbackoff.
- OCPBUGS-38940 - [4.14] Ironic issues soft power_off command during installation via ACM, preventing fakefish from working on certain configurations
- OCPBUGS-38972 - PAC: PLRs log link is broken
- OCPBUGS-39413 - az.EnsureHostInPool panic when Azure VM instance not found

CVEs

- CVE-2022-23772
- CVE-2023-6597
- CVE-2023-31315
- CVE-2023-37920
- CVE-2023-45142
- CVE-2023-45288
- CVE-2023-45539
- CVE-2023-47108
- CVE-2023-48795
- CVE-2024-0874
- CVE-2024-1737
- CVE-2024-1975
- CVE-2024-2398
- CVE-2024-4076
- CVE-2024-6104
- CVE-2024-6345
- CVE-2024-26946
- CVE-2024-34069
- CVE-2024-35839
- CVE-2024-35875

- CVE-2024-35895
- CVE-2024-37370
- CVE-2024-37371
- CVE-2024-37891
- CVE-2024-38428
- CVE-2024-38476
- CVE-2024-38540
- CVE-2024-38570
- CVE-2024-39502
- CVE-2024-40914
- CVE-2024-40956
- CVE-2024-40978
- CVE-2024-40983
- CVE-2024-41044
- CVE-2024-42102
- CVE-2024-42131

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

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
Cookie preferences