RHSA-2024:7922 - Security Advisory

Issued: 2024-10-16 Updated: 2024-10-16

Synopsis

Important: OpenShift Container Platform 4.17.1 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.17.1 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 4.17.1. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2024:7925

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/4.17/release_notes/ocp-4-17-release-notes.html

Security Fix(es):

- pypa/setuptools: Remote code execution via download functions in the

package_index module in pypa/setuptools (CVE-2024-6345)

- openshift-console: OAuth2 insufficient state parameter entropy

(CVE-2024-6508)

- Hashicorp/vault: Vault's LDAP Auth Method Allows for User Enumeration

(CVE-2023-3462)

- golang: net/http: golang: mime/multipart: golang: net/textproto: memory

exhaustion in Request.ParseMultipartForm (CVE-2023-45290)

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

(CVE-2024-3727)

- golang-protobuf: encoding/protojson, internal/encoding/json: infinite

loop in protojson.Unmarshal when unmarshaling certain forms of invalid JSON
(CVE-2024-24786)

- net/http: Denial of service due to improper 100-continue handling in

net/http (CVE-2024-24791)

- pgx: SQL Injection via Line Comment Creation (CVE-2024-27289)
- path-to-regexp: Backtracking regular expressions cause ReDoS

(CVE-2024-45296)

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.openshift.com/container-platform/4.17/updating/updating_a_cluster/updating-cluster-cli.html

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.openshift.com/container-platform/4.17/release_notes/ocp-4-17-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:e16ac60ac6971e5b6f89c1d818f5ae711c0d63ad6a6a26ffe795c738e8cc4dde

(For s390x architecture)
The image digest is
sha256:c3372900c1b249fc1fa017db9ddcfa2b97a71a358e8d377481e0ca04a9d121d3

(For ppc64le architecture)
The image digest is
sha256:fec4a60f96ad4c29ff2d4401fa079c5b1e0af05b0914cae2b8d29ff026654d95

(For aarch64 architecture)
The image digest is
sha256:62b77793b08477b7c785ac0fab76f919bed8cf31c1bf4678da4df03b8c2a7a58

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.openshift.com/container-platform/4.17/updating/updating_a_cluster/updating-cluster-cli.html

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 - 2228020 - CVE-2023-3462 Hashicorp/vault: Vault?s LDAP Auth Method Allows for User Enumeration
- BZ - 2268017 - CVE-2023-45290 golang: net/http: golang: mime/multipart: golang: net/textproto: memory exhaustion in Request.ParseMultipartForm
- BZ - 2268046 - CVE-2024-24786 golang-protobuf: encoding/protojson, internal/encoding/json: infinite loop in protojson.Unmarshal when unmarshaling certain forms of invalid JSON
- BZ - 2268465 - CVE-2024-27289 pgx: SQL Injection via Line Comment Creation
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2295310 - CVE-2024-24791 net/http: Denial of service due to improper 100-continue handling in net/http
- BZ - 2295777 - CVE-2024-6508 openshift-console: OAuth2 insufficient state parameter entropy
- BZ - 2297771 - CVE-2024-6345 pypa/setuptools: Remote code execution via download functions in the package_index module in pypa/setuptools
- BZ - 2310908 - CVE-2024-45296 path-to-regexp: Backtracking regular expressions cause ReDoS
- OCPBUGS-30950 - ovnkube-node hostPath mount of /var/lib/kubelet is missing HostToContainer mountPropagation, breaks CSI driver
- OCPBUGS-33815 - openshift-controller-manager overwriting/undoing changes to ServiceAccount imagePullSecrets
- OCPBUGS-33834 - openshift-controller-manager pod panic due to type assertion
- OCPBUGS-33899 - ART requests updates to 4.17 image ose-cluster-samples-operator-container
- OCPBUGS-34034 - ART requests updates to 4.17 image ose-cluster-bootstrap-container
- OCPBUGS-34073 - ART requests updates to 4.17 image ose-olm-rukpak-container
- OCPBUGS-34134 - ART requests updates to 4.17 image ose-agent-installer-api-server-container
- OCPBUGS-34217 - ART requests updates to 4.17 image ose-csi-driver-shared-resource-container
- OCPBUGS-34285 - ART requests updates to 4.17 image ose-network-metrics-daemon-container
- OCPBUGS-34314 - ART requests updates to 4.17 image aws-kms-encryption-provider-container

- OCPBUGS-34643 - metrics do not show up at openshift console
- OCPBUGS-35430 - PowerVS: Query the CAPI provider for the timeouts needed during provisioning
- OCPBUGS-35868 - ART requests updates to 4.17 image ose-sriov-network-metrics-exporter-container
- OCPBUGS-36213 - webhook service is missed in openshift-console-operator namespace
- OCPBUGS-36680 - The change of the additionalTrustBundle doesn't propagate to worker node.
- OCPBUGS-38240 - Disable "Helm release status verification: HR-01-TC04" test due to CI outage
- OCPBUGS-38379 - Enable MSI override for Image Registry is Missing
- OCPBUGS-38457 - Manila driver and node-registrar does not uses healtcheck
- OCPBUGS-38462 - 2 Metrics tab in 4.17 developer console
- OCPBUGS-38471 - [cluster-samples-operator] [4.17] Only update the supported samples during release prep
- OCPBUGS-38563 - [release-4.17] Directly mutating links in useMemo may not result in re-render
- OCPBUGS-38574 - [4.17] use pooled client for etcd single member health checks
- OCPBUGS-38760 - CAPZ empty route table created during install
- OCPBUGS-38770 - [4.17.z] SCC pinning for all workloads in platform namespaces (openshift-*-infra)
- OCPBUGS-38784 - [4.17] redfish-virtualmedia fails on xFusion nodes
- OCPBUGS-38927 - [cluster-samples-operator][4.17] Bump Kubernetes Version 29.2 to latest stable API
- OCPBUGS-39013 - Ironic inspection fails due to utf-8 decoding issue on Disk serial
- OCPBUGS-39071 - [cluster-samples-operator][4.17] Fix library-sync.sh to handle renames correctly
- OCPBUGS-39091 - [release-4.17] clear all filters button is counted into resource type number
- OCPBUGS-39120 - [cluster-samples-operator][4.17] Update the supported samples from openshift/library
- OCPBUGS-39124 - Failure to pull NTO image preventing startup of ocp-tuned-one-shot.service
- OCPBUGS-39286 - UPI playbook failing due to missing metadata.json
- OCPBUGS-39390 - Fix lists sorting
- OCPBUGS-42081 - In OCB, "enforcing=0" kernel argument is degrading the MachineConfigPool
- OCPBUGS-42098 - HostedClusterConfigOperator used wrong certificate for Kube certificate authority
- OCPBUGS-42116 - GCP Principal remains in Host project

- OCPBUGS-42126 - [IBMCloud] update the "Tested instance types for IBMCloud"
- OCPBUGS-42131 - The CI job e2e-gcp keeps failing in openshift/network-metrics-daemon
- OCPBUGS-42142 - [GCP] installing into GCP shared VPC with BYO hosted zone failed with error "failed to create the private managed zone"
- OCPBUGS-42164 - oc adm prune deployments` does not work and giving panic when using --replica-set option
- OCPBUGS-42200 - MCPs report wrong number of nodes when we move nodes from one custom MCP to another custom MCP
- OCPBUGS-42223 - [release-4.17] The highlighted lines for "Hide Lightspeed" is shown on top of Lightspeed popup modal.
- OCPBUGS-42232 - openshift-apiserver panicked with runtime error
- OCPBUGS-42248 - Sort function on NetworkPolicies page is incorrect after enable Pagination
- OCPBUGS-42256 - Panic seen in CI job for MCC pod
- OCPBUGS-42261 - Hypershift is managing kubeconfigs for DNS and Ingress operators
- OCPBUGS-42277 - [IBMCloud] MonitorTests fail due to CSI Driver pods require ClusterRole SCC binding
- OCPBUGS-42296 - Azure: installation failed when controlPlane.platform is empty in install-config
- OCPBUGS-42323 - IRQBALANCE_BANNED_CPUS is not updated with isolated cpus when irq load balancing is disabled
- OCPBUGS-42336 - [4.17] Fix ImageEcosystem tests
- OCPBUGS-42357 - [release-4.17]RemoteConfiguration clusteroperator conditions reporting as available in disabled cluster
- OCPBUGS-42362 - Continuous pull-secret updates / slow initialization on build01 (test platform infrastructure)
- OCPBUGS-42380 - [4.17] Monitoring should be enabled by default when installing OpenShift Lightspeed
- OCPBUGS-42394 - Azure private account setup with vnet discovery fails to find vnet by tag
- OCPBUGS-42410 - [release-4.17] Update rhel base image to rhel 9 for ansible-operator image
- OCPBUGS-42421 - [release-4.17] oc-mirror skips images with digest and tag
- OCPBUGS-42483 - PowerVS update capi ibmcloud c6bcd313 for 4.17
- OCPBUGS-42580 - Node ISO Missing <arch> in the created filename
- OCPBUGS-42581 - ?Edit Route? should support Form edit
- OCPBUGS-42582 - "router's" should be "router's" on route creation page.
- OCPBUGS-42585 - RedHat CamelK operator installation through CLI
- OCPBUGS-42606 - Unable to create alert silence in developer UI though "Creator" field is NOT mandatory
- OCPBUGS-42612 - cluster-api-operator not sync with upstream version missing features

- OCPBUGS-42622 - could not install cli-manager-operator on arm64 clusters
- OCPBUGS-42677 - The MCO does not properly degrade when pools are failing to render a new config
- OCPBUGS-42678 - Service name field should not use id "toggle-host".
- OCPBUGS-42681 - user is unable to edit Weight for the first selected Service
- OCPBUGS-42699 - Extra control plane VMs created during GCP install in 4.17+
- OCPBUGS-42714 - OAuthServer service with Route type does not work with a custom hostname
- OCPBUGS-42721 - oc command won't mirror images with different name, but same layers
- OCPBUGS-42786 - Update base image of scaffolded Dockerfile for helm-operator to use rhel9 repository
- OCPBUGS-42812 - Errors when the image registry is configured to use a custom Azure storage account located in a different resource group blocked the upgrade
- OCPBUGS-42814 - Samples Operator Sync Breaks Build Suite Tests
- OCPBUGS-42853 - Update base image of scaffolded Dockerfile for ansible-operator to use rhel9 repository
- OCPBUGS-39409 - UPI playbooks when master schedulable fails
- OCPBUGS-39414 - CI doesn't reflect software used during tests
- OCPBUGS-39601 - Console user settings resources misses ownerRef, removing a user results in remaining data
- OCPBUGS-41255 - Configure-ovs doesn't persist ethtool configuration
- OCPBUGS-41341 - user workload monitoring is trying to scrap RH operators which have been installed in openshift-operators namespace
- OCPBUGS-41357 - Supporting Bridge Type Linux Interfaces for Primary Networking
- OCPBUGS-41376 - subscription-manager is needed to make dnf useful
- OCPBUGS-41576 - [capi] sometimes cluster-capi-operator pod stuck in CrashLoopBackOff on osp
- OCPBUGS-41622 - [4.17] Bootimage bump tracker
- OCPBUGS-41685 - Topology screen crashes when completed pod is selected
- OCPBUGS-41686 - MCPs with RHEL nodes are degraded when a userCA bundle is added to the cluster
- OCPBUGS-41817 - "pods should successfully create sandboxes by adding pod to network" are failing on multiple platforms
- OCPBUGS-41893 - Disable Extension Catalog navigation item
- OCPBUGS-41908 - Alerts with a non-standard severity label should be filtered out from Telemetry
- OCPBUGS-41914 - [release-4.17] https://console.redhat.com/api/gathering/v2/%s/gathering_rules should have %s populated
- OCPBUGS-41933 - Cloud Event API GET CurrentState has extra '/' in ResourceAddress
- OCPBUGS-41941 - [IBMCloud] CCM liveness probe in failure loop

- OCPBUGS-42006 - cns-migration tool doesn't checks for vcenter version before starting migration
- OCPBUGS-42007 - Removed vSphere CSI driver leaves lot of conditions
- OCPBUGS-42008 - cns-migration exits logic enhancement
- OCPBUGS-42019 - [OCP-4.17] Creating pod with the safe sysctls configuration failed for non-privileged users
- OCPBUGS-42060 - Console crashes when ssh is selected in add secret for starting a pipeline run
- OCPBUGS-42066 - Speed up CMO e2e tests [4.17]

CVEs

- CVE-2021-47385
- CVE-2022-24805
- CVE-2022-24806
- CVE-2022-24807
- CVE-2022-24808
- CVE-2022-24809
- CVE-2022-24810
- CVE-2023-3462
- CVE-2023-20584
- CVE-2023-28746
- CVE-2023-31356
- CVE-2023-45290
- CVE-2023-52439
- CVE-2023-52658
- CVE-2023-52884
- CVE-2024-3727
- CVE-2024-6119
- CVE-2024-6345
- CVE-2024-6508
- CVE-2024-7383
- CVE-2024-9341
- CVE-2024-24786
- CVE-2024-24791
- CVE-2024-26739
- CVE-2024-26929
- CVE-2024-26930
- CVE-2024-26931
- CVE-2024-26947
- CVE-2024-26991
- CVE-2024-27022

- CVE-2024-27289
- CVE-2024-27403
- CVE-2024-34156
- CVE-2024-35895
- CVE-2024-35989
- CVE-2024-36016
- CVE-2024-36889
- CVE-2024-36899
- CVE-2024-36978
- CVE-2024-38556
- CVE-2024-38562
- CVE-2024-38570
- CVE-2024-38573
- CVE-2024-38601
- CVE-2024-38615
- CVE-2024-39483
- CVE-2024-39502
- CVE-2024-40959
- CVE-2024-40984
- CVE-2024-41071
- CVE-2024-42079
- CVE-2024-42225
- CVE-2024-42246
- CVE-2024-42272
- CVE-2024-42284
- CVE-2024-42353
- CVE-2024-45296
- CVE-2024-45490
- CVE-2024-45491
- CVE-2024-45492
- CVE-2024-45769
- CVE-2024-45770

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

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