RHSA-2025:3301 - Security Advisory

Issued: 2025-04-03 Updated: 2025-04-03

Synopsis

Important: OpenShift Container Platform 4.16.38 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.16.38 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 4.16.

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

https://access.redhat.com/errata/RHBA-2025:3303

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/4.16/html/release_notes/

Security Fix(es):

- buildah: Buildah allows arbitrary directory mount (CVE-2024-9675)
- kernel: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy

and Mbox devices (CVE-2024-53197)

- libxml2: Use-After-Free in libxml2 (CVE-2024-56171)
- grub2: net: Out-of-bounds write in grub_net_search_config_file()

(CVE-2025-0624)

- libxml2: Stack-based buffer overflow in xmlSnprintfElements of libxml2

(CVE-2025-24928)

- Podman: Buildah: CRI-O: symlink traversal vulnerability in the

containers/storage library can cause Denial of Service (DoS)
(CVE-2024-9676)

- github.com/moby/moby: NULL Pointer Dereference in Moby (CVE-2024-36620)
- kernel: HID: core: zero-initialize the report buffer (CVE-2024-50302)
- go-jose: Go JOSE's Parsing Vulnerable to Denial of Service

(CVE-2025-27144)

All OpenShift Container Platform 4.16 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/4.16/html-single/updating_clusters/index#updating-cluster-cli.

Solution

For OpenShift Container Platform 4.16 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/4.16/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
sha256:6da09834a9e0e30a79f77c13c2520a25172d8be3fc044dc2ad1392d69b2edfbf

(For s390x architecture)
The image digest is
sha256:bcd96f1db1a6dcf6f7185d5410d9d665fb72545b1094c5d4e5696e08c10e0adf

(For ppc64le architecture)
The image digest is
sha256:30f50074efde956337703e02c05a8a47854a669745178684ab9e18ca38173278

(For aarch64 architecture)
The image digest is
sha256:0b83c98681f690f8c45c0f13002c251b925023da9416bf3106f9e9aeeec810ef

All OpenShift Container Platform 4.16 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/4.16/html-single/updating_clusters/index#updating-cluster-cli.

Affected Products

- Red Hat OpenShift Container Platform 4.16 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 9 aarch64

Fixes

- BZ - 2317458 - CVE-2024-9675 buildah: Buildah allows arbitrary directory mount
- BZ - 2317467 - CVE-2024-9676 Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS)
- BZ - 2327169 - CVE-2024-50302 kernel: HID: core: zero-initialize the report buffer

- BZ - 2329534 - CVE-2024-36620 github.com/moby/moby: NULL Pointer Dereference in Moby
- BZ - 2334412 - CVE-2024-53197 kernel: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy and Mbox devices
- BZ - 2346112 - CVE-2025-0624 grub2: net: Out-of-bounds write in grub_net_search_config_file()
- BZ - 2346416 - CVE-2024-56171 libxml2: Use-After-Free in libxml2
- BZ - 2346421 - CVE-2025-24928 libxml2: Stack-based buffer overflow in xmlSnprintfElements of libxml2
- BZ - 2347423 - CVE-2025-27144 go-jose: Go JOSE's Parsing Vulnerable to Denial of Service
- OCPBUGS-42960 - [release-4.16] OSUS: create a must-gather image to collect OSUS specific data
- OCPBUGS-44622 - VolumeAttachment does not reconcile on worker VM reboot
- OCPBUGS-44674 - Allow from host network netpol doesn't work because flows in table 80 are not created against VNID 0
- OCPBUGS-46388 - 4.15/4.16 developer console, Alerting rule link is broken
- OCPBUGS-46466 - Cannot access external network via https from the HCP openshift-apiserver component
- OCPBUGS-49409 - ERROR in search tool: Cannot read properties of undefined (reading 'state')
- OCPBUGS-49696 - OpenShift internal registry panic when deploying OpenShift on AWS ap-southeast-5 region
- OCPBUGS-49800 - Function Import: An error occurred Cannot read properties of undefined (reading 'filter')
- OCPBUGS-49906 - Bump to kubernetes 1.29.14
- OCPBUGS-49979 - OCP sample application don't create BuildConfig resource
- OCPBUGS-50590 - Upgrade failing because custom scc in version pod
- OCPBUGS-50594 - [4.16z] Pod running on a node on which egress IPv6 is assigned, not able to communicate with k8s service in a dual stack cluster.
- OCPBUGS-50966 - [azure] Worker machines get Failed state if region has no availability zones or availability set fault domains
- OCPBUGS-50993 - HyperShift Control Plane Operator doesn't honor proxy env variable in some places
- OCPBUGS-51043 - oc debug node doesn't setup the right environment for sosreport
- OCPBUGS-51074 - Error while creating the egressfirewall dnsName with uppercase on OCP 4.16
- OCPBUGS-51206 - RHOCP 4.16 upgrade blocker - kubernetes-sigs#3015 cherry-pick request for the vsphere-csi-driver
- OCPBUGS-51207 - Validation status logs contain wrong hostname

- OCPBUGS-51346 - Assisted Installer Agent image pull timeout is too short
- OCPBUGS-51362 - 4.17 Failed workers reboot in HA topology prevents cluster deployment completion
- OCPBUGS-52191 - [release-4.16] cluster failed installation in aws with ap-southeast-5 region
- OCPBUGS-52252 - dev console, click Description link in "Alerting rule details" page, "No Alert found" shows
- OCPBUGS-52288 - While upgrading the cluster from UI observed `Warning alert:Admission Webhook Warning`
- OCPBUGS-52310 - ovs-configuration failed to start after reboot
- OCPBUGS-52329 - DeletionCandidateOfClusterAutoscaler taints not getting removed
- OCPBUGS-52342 - oVirt support should be removed from Machine API operator
- OCPBUGS-52404 - nmstate: after reboot wait-for-br-ex-up.service stuck
- OCPBUGS-52418 - [release-4.16] While accessing the node terminal from UI observed 'Warning alert:Admission Webhook Warning`
- OCPBUGS-52426 - Typo in log message for keyword "Platform" in hypershift operator logs.
- OCPBUGS-52450 - [release-4.16] Oh no! Something went wrong error occurs when cluster settings is accessed.
- OCPBUGS-52498 - [release-4.16] Add runbook_url for CoreDNSErrorsHigh
- OCPBUGS-52593 - Unexpected Permissions in `cluster-reader` ClusterRole in OpenShift 4.16
- OCPBUGS-52851 - Show Observe section without PROMETHEUS and MONITORING flags
- OCPBUGS-52857 - The trusted-ca-bundle-managed ConfigMap requirement breaks those with their own PKI
- OCPBUGS-53313 - Race condition in rpm-ostree update logic
- OCPBUGS-53459 - [AWS CAPI install] Failed to create C2S/SC2S cluster via Cluster API

CVEs

- CVE-2022-49043
- CVE-2024-9675
- CVE-2024-9676
- CVE-2024-36620
- CVE-2024-50302
- CVE-2024-53197
- CVE-2024-56171
- CVE-2025-0624
- CVE-2025-1244
- CVE-2025-22869
- CVE-2025-24201
- CVE-2025-24928
- CVE-2025-27144

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 Summit
