



Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

4-10-24

RHSA

Advis

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Overview

Updated In

Synop

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Importan

Type/

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Security

Topic

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Red Hat

images t

This rele

ges and

Red Hat


Clearing your browser cookies may delete your cookie preferences. If you re- 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.

Common


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

<https://access.redhat.com/errata/RHSA-2024:8263> 

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/4.16/release_notes/ocp-4-16-release-notes.html 


Security Fix(es):

- encoding/gob: golang: Calling Decoder.Decode on a message which contains

deeply nested structures can cause a panic due to stack exhaustion (CVE-2024-34156)

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

(CVE-2024-3727)

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

net/http (CVE-2024-24791)


- jose-go: improper handling of highly compressed data (CVE-2024-28180)
- go/parser: golang: Calling any of the Parse functions containing deeply

nested literals can cause a panic/stack exhaustion (CVE-2024-34155)

- go/build/constraint: golang: Calling Parse on a "// +build" build tag


line with deeply nested expressions can cause a panic due to stack exhaustion (CVE-2024-34158)


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 4.16 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.openshift.com/container-platform/4.16/updating/updating_a_cluster/updating-cluster-cli.html 

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.openshift.com/container-platform/4.16/release_notes/ocp-4-16-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 as follows:

(For x86_64 architecture)

The image digest is

sha256:3f14e29f5b42e1fee7d7e49482cfff4df0e63363bb4a5e782b65c66aba4944e7

(For s390x architecture)

The image digest is

sha256:539069342e21f9a41efa9fe21003e478cf548a1ecd591adadae3b3514bfdff2d

(For ppc64le architecture)


The image digest is

sha256:9ea793675dc34a2924887d4cbe2e0ff70d26679f1b3e1785ae6c6ba73cdc826

(For aarch64 architecture)

The image digest is sha256:




bcbade4f6aa446a3501f7ebc1a80d2e21369d5d1cfe0609b386a9f2512e42c77























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.openshift.com/container-platform/4.16/updating/updating_a_cluster/updating-cluster-cli.html 

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 - 2268854](#)  - CVE-2024-28180 jose-go: improper handling of highly compressed data
- [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 - 2310527](#)  - CVE-2024-34155 go/parser: golang: Calling any of the Parse functions containing deeply nested literals can cause a panic/stack exhaustion
- [BZ - 2310528](#)  - CVE-2024-34156 encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion
- [BZ - 2310529](#)  - CVE-2024-34158 go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion
- [OCPBUGS-33692](#)  - ART requests updates to 4.16 image azure-kms-encryption-provider-container
- [OCPBUGS-33693](#)  - ART requests updates to 4.16 image aws-kms-encryption-provider-container
- [OCPBUGS-39415](#)  - CI doesn't reflect software used during tests
- [OCPBUGS-41364](#)  - PTP events loses connectivity between producer and consumer when external interface is lost
- [OCPBUGS-41805](#)  - [4.16.z] SCC pinning for all workloads in platform namespaces (metallb-operator)
- [OCPBUGS-41904](#)  - NAD created for ovn-k8s-cni-overlay via console form is unusable
- [OCPBUGS-42014](#)  - Cluster creation failure rate increased since June 2024
- [OCPBUGS-42369](#)  - Console crashes when ssh is selected in add secret for starting a pipeline run
- [OCPBUGS-42420](#)  - Continuous pull-secret updates / slow initialization on build01 (test platform infrastructure)
- [OCPBUGS-42432](#)  - HostedClusterConfigOperator used wrong certificate for Kube certificate authority
- [OCPBUGS-42724](#)  - openshift-apiserver panicked with runtime error
- [OCPBUGS-42933](#)  - Errors when the image registry is configured to use a custom Azure storage account located in a different resource group blocked the upgrade
- [OCPBUGS-43056](#)  - gather_network_logs_basics script when node is in the NotReady [backport 4.16]
- [OCPBUGS-43063](#)  - Router should support SHA-1 CA certificates in the default certificate chain
- [OCPBUGS-43104](#)  - OAuthServer service with Route type does not work with a custom hostname
- [OCPBUGS-43105](#)  - [operator-sdk] FIPS scan failed
- [OCPBUGS-43308](#)  - HCP unable to pull images from registries only accessible from worker nodes
- [OCPBUGS-43433](#)  - [vsphere] Machine stuck in Provisioning status when machine is power off
- [OCPBUGS-43467](#)  - Load Red Hat keys in FIPS mode with Go 1.22

CVEs

- [CVE-2024-3727](#) 

- [CVE-2024-9341](#)
- [CVE-2024-23271](#)
- [CVE-2024-24791](#)
- [CVE-2024-27820](#)
- [CVE-2024-27838](#)
- [CVE-2024-27851](#)
- [CVE-2024-28180](#)
- [CVE-2024-34155](#)
- [CVE-2024-34156](#)
- [CVE-2024-34158](#)
- [CVE-2024-40776](#)
- [CVE-2024-40779](#)
- [CVE-2024-40780](#)
- [CVE-2024-40782](#)
- [CVE-2024-40789](#)
- [CVE-2024-40866](#)
- [CVE-2024-44187](#)

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](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Opt-Out Rights](#)