



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.

RHSA

24-10-31

Overview

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.

Updated P

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.

Importa

Type/

Security

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.

| |
|--------------|
| Red H |
| Identifi |
| View a |

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".

Topic

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your

Red Hat

preferences at that time. If you have set your browser's global privacy

ages and

images that fix several bugs and add enhancements.


This release includes a security update for Red Hat OpenShift Container Platform 4.15.

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 RPM packages for Red Hat OpenShift Container Platform 4.15.37. See the following advisory for the container images for this release:

<https://access.redhat.com/errata/RHSA-2024:8425> 

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)
- Podman: Buildah: cri-o: FIPS Crypto-Policy Directory Mounting Issue in containers/common Go Library (CVE-2024-9341)
- Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS) (CVE-2024-9676)
- 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 4.15 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/4.15/updating/updating_a_cluster/updating-cluster-cli.html 

Solution

For OpenShift Container Platform 4.15 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/4.15/release_notes/ocp-4-15-release-notes.html

Affected Products

- Red Hat OpenShift Container Platform 4.15 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.15 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 8 aarch64

Fixes

- [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
- [BZ - 2315691](#) - CVE-2024-9341 Podman: Buildah: cri-o: FIPS Crypto-Policy Directory Mounting Issue in containers/common Go Library
- [BZ - 2317467](#) - CVE-2024-9676 Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS)



CVEs


- [CVE-2024-9341](#)
- [CVE-2024-9676](#)
- [CVE-2024-34155](#)
- [CVE-2024-34156](#)
- [CVE-2024-34158](#)


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](#)