



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

4-09-16

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.

Moderat

Type/Severity

Security Advisory: Moderate

Topic

Updated images are now available for Red Hat Advanced Cluster Security for Kubernetes (RHACS). The updated image includes security and bug fixes.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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

This release of RHACS 4.5.2 includes the security fix for the following CVE:

- containers/image: digest type does not guarantee valid type (CVE-2024-3727)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

This release of RHACS fixes the following bugs:

- Fixed an issue where Sensor was unable to identify OpenShift Container Platform internal registry secrets due to a change in the pull secret annotation.
- Fixed an issue where policies incorrectly displayed an enforced value of Yes in the Configuration Management -> Application & Infrastructure -> Deployments page due to inconsistent status handling, while showing No in the Violations page.
- Fixed an issue where vulnerability data differed between the Vulnerability Management Workload CVE pages and the deprecated Vulnerability Management dashboard due to inconsistencies in vulnerability reporting.

Solution

If you are using an earlier version of RHACS 4.5, you are advised to upgrade to this patch release 4.5.2.

Affected Products

- Red Hat Advanced Cluster Security for Kubernetes 4 x86_64
- Red Hat Advanced Cluster Security for Kubernetes for IBM Z and LinuxONE 4 s390x
- Red Hat Advanced Cluster Security for Kubernetes for IBM Power, little endian 4 ppc64le

Fixes

- [BZ - 2274767](#) - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- [ROX-26147](#) - Release RHACS 4.5.2

CVEs

- [CVE-2024-1737](#)
- [CVE-2024-1975](#)
- [CVE-2024-2398](#)
- [CVE-2024-3727](#)
- [CVE-2024-6345](#)
- [CVE-2024-37370](#)
- [CVE-2024-37371](#)
- [CVE-2024-37891](#)

References

- <https://access.redhat.com/security/updates/classification/#moderate>
- https://docs.openshift.com/acs/4.5/release_notes/45-release-notes.html

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 

 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](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

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