RHSA-2026:0627 - Security Advisory

Issued: 2026-01-14 Updated: 2026-01-14

Overview

Updated Images

Synopsis

Important: Red Hat Advanced Cluster Management for Kubernetes v2.13.5 security update

Type/Severity

Security Advisory: Important

Topic

Red Hat Advanced Cluster Management for Kubernetes 2.13 General Availability release images, which add new features and enhancements, bug fixes, and updated container images.

Description

Red Hat Advanced Cluster Management for Kubernetes 2.13 images

Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console—with security policy built in.

This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which add new features and enhancements, bug fixes, and updated container images. See the following Release Notes documentation, which will be updated shortly for this release, for additional details about this release:

https://docs.redhat.com/en/documentation/red_hat_advanced_cluster_management_for_kubernetes/2.13/html-single/release_notes/index#acm-release-notes

Solution

Before you apply this update, make sure all previously released errata that are relevant to your system are applied.

For details on how to apply this update, refer to:

https://access.redhat.com/articles/11258

Fixes

- ACM-22364 - [ACM 2.13] The Repository/Source Code link for the operator is missing from the operator installation/overview window.
- ACM-23944 - ACM console shows updates for HCP BareMetal clusters but upgrade option is greyed out despite valid channel configuration 2.13
- ACM-24089 - [2.13] ApplicationSubscription unable to handle Kustomization from ObjectBucket Channel
- ACM-24721 - console-mce pod CrashLoopBackOff due to probe failure [release-2.13]
- ACM-24922 - [2.13] Using multiple metric-collector workers may cause loss of metrics due to race condition
- ACM-27638 - console-mce-console readiness and liveness probe failures at scale during ACM ZTP with AAP and EDA

CVEs

- CVE-2025-27144
- CVE-2025-47907
- CVE-2025-58183
- CVE-2025-58754
- CVE-2025-7195
- CVE-2025-9287
- CVE-2025-9288

References

- https://access.redhat.com/security/updates/classification/
- 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

Loading

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