RHSA-2025:17562 - Security Advisory

Issued: 2025-10-08 Updated: 2025-10-08

Synopsis

Moderate: AMQ Broker 7.13.2.OPR.1.GA Container Images release and security update

Type/Severity

Security Advisory: Moderate

Topic

This is the multiarch release of the AMQ Broker 7.13.2 aligned Operator and associated container images on Red Hat Enterprise Linux for the OpenShift Container Platform.

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

Red Hat Middleware for OpenShift provides images for many of the Red Hat Middleware products for use within the OpenShift Container Platform cloud computing Platform-as-a-Service (PaaS) for on-premise or private cloud deployments.

This release of Red Hat AMQ Broker 7.13.2 includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Security Fix(es):

- (CVE-2025-58712) amq-broker-init-rhel9: privilege escalation via excessive /etc/passwd permissions
- (CVE-2025-58712) amq-broker-rhel9: privilege escalation via excessive /etc/passwd permissions

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.

For information on supported configurations, see Red Hat AMQ Broker 7 Supported Configurations at https://access.redhat.com/articles/2791941

Solution

To update to the latest image please refer to the AMQ container images in the Red Hat Container catalog.

Affected Products

- Red Hat OpenShift Container Platform 4.12 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.11 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.10 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.9 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.7 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.6 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.5 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.4 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.3 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.2 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.1 for RHEL 8 x86_64
- Red Hat JBoss Middleware 1 x86_64
- Red Hat OpenShift Container Platform for Power 4.10 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.9 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.7 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.6 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.5 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.4 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.3 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.10 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.9 for RHEL 8 s390x

- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.8 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.7 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.6 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.5 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.4 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.3 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.2 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.10 aarch64

Fixes

- BZ - 2394418 - CVE-2025-58712 amq: privilege escalation via excessive /etc/passwd permissions

CVEs

- CVE-2022-29458
- CVE-2024-47081
- CVE-2025-5914
- CVE-2025-6020
- CVE-2025-6395
- CVE-2025-8058
- CVE-2025-8194
- CVE-2025-8941
- CVE-2025-32414
- CVE-2025-32415
- CVE-2025-32988
- CVE-2025-32989
- CVE-2025-32990
- CVE-2025-58712

References

- https://access.redhat.com/security/updates/classification/#moderate
- https://access.redhat.com/security/updates/classification#moderate
- https://docs.redhat.com/en/documentation/red_hat_amq_broker/

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

⚠ 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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility