RHSA-2025:22724 - Security Advisory

发布： 2025-12-10 已更新： 2025-12-10

概述

概述

Important: OpenShift Container Platform 4.16.54 bug fix and security update

类型/严重性

Security Advisory: Important

标题

Red Hat OpenShift Container Platform release 4.16.54 is now available with updates to packages and images that fix several bugs and add enhancements.

This release includes a security update for Red Hat OpenShift Container Platform 4.16.

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.

描述

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

https://access.redhat.com/errata/156901

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.redhat.com/en/documentation/openshift_container_platform/4.16/html/release_notes/

Security Fix(es):

- sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems (CVE-2025-11561)
- podman: Build Context Bind Mount (CVE-2025-4953)

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.redhat.com/en/documentation/openshift_container_platform/4.16/html-single/updating_clusters/index#updating-cluster-cli.

解决方案

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.redhat.com/en/documentation/openshift_container_platform/4.16/html/release_notes/

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
sha256:5efb10e511ff6623fee08dd8cfa8915b9be5cc3b7f7501731ddc13fa0d2ea988

(For s390x architecture)
The image digest is
sha256:2b77c206c6ab23808a1b3988f7e87f4dae14dbc57bf300e1ce1eabc945667b64

(For ppc64le architecture)
The image digest is
sha256:6cbdd40976744d791db379a0c6d1a4203a17cf0f31a865e19916025647b7244a

(For aarch64 architecture)
The image digest is
sha256:c71acfbc01a33e3cce8f02f3f2354409c3a00bfdaa46f0b4f53ac8ee8e763d8a

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.redhat.com/en/documentation/openshift_container_platform/4.16/html-single/updating_clusters/index#updating-cluster-cli.

受影响的产品

- 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

修复

- BZ - 2367235 - CVE-2025-4953 podman: Build Context Bind Mount
- BZ - 2402727 - CVE-2025-11561 sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems

CVE

- CVE-2025-4953
- CVE-2025-11561

参考

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

---

Red Hat 安全团队联络方式为 secalert@redhat.com。 更多联络细节请参考 https://access.redhat.com/security/team/contact/。

Red Hat

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility