

[Subscriptions](#) | [Downloads](#) | [Red Hat Console](#) | [Get Support](#)

Red Hat F

# RHSA Advis

6-01-07

[Overview](#)

## Synop

Importa

## Type/

Security Advisory: Important

## Topic

Red Hat OpenShift Container Platform release 4.15.60 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 4.15.

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 container images for Red Hat OpenShift Container Platform 4.15.60. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/157173> [↗](#)

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/4.15/html/release\\_notes/](https://docs.redhat.com/en/documentation/openshift_container_platform/4.15/html/release_notes/)  
↗

#### Security Fix(es):

- sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems (CVE-2025-11561)
- runc: container escape via 'masked path' abuse due to mount race conditions (CVE-2025-31133)
- runc: container escape with malicious config due to /dev/console mount and related races (CVE-2025-52565)
- runc: opencontainers/selinux: container escape and denial of service due to arbitrary write gadgets and procfs write redirects (CVE-2025-52881)
- 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 4.15 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.redhat.com/en/documentation/openshift\\_container\\_platform/4.15/html-single/updating\\_clusters/index#updating-cluster-cli](https://docs.redhat.com/en/documentation/openshift_container_platform/4.15/html-single/updating_clusters/index#updating-cluster-cli). ↗

## 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.redhat.com/en/documentation/openshift\\_container\\_platform/4.15/html/release\\_notes/](https://docs.redhat.com/en/documentation/openshift_container_platform/4.15/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

sha256:39236e073ff4b62406a472178263fd2220b0f544c3fd26036120b470596fa255

(For s390x architecture)

The image digest is

sha256:f94d7fce531623dd0d1d4b5fe1c299eba7152676306ed2e9ea3c7fe17b4ad5ee

(For ppc64le architecture)

The image digest is

sha256:5cdc5d1a0cb3b990afb8d1559abf87d9194c375541f27689aa974c1336d9eb

(For aarch64 architecture)

The image digest is

sha256:584bb60432b0460d97b9624a3cb1c625469534ac44dedb618f14834161c2d448

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.redhat.com/en/documentation/openshift\\_container\\_platform/4.15/html-single/updating\\_clusters/index#updating-cluster-cli](https://docs.redhat.com/en/documentation/openshift_container_platform/4.15/html-single/updating_clusters/index#updating-cluster-cli). [↗](#)

## 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 - 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
- BZ - 2404705 [↗](#) - CVE-2025-31133 runc: container escape via 'masked path' abuse due to mount race conditions
- BZ - 2404708 [↗](#) - CVE-2025-52565 runc: container escape with malicious config due to /dev/console mount and related races
- BZ - 2404715 [↗](#) - CVE-2025-52881 runc: opencontainers/selinux: container escape and denial of service due to arbitrary write gadgets and procfs write redirects

## CVEs

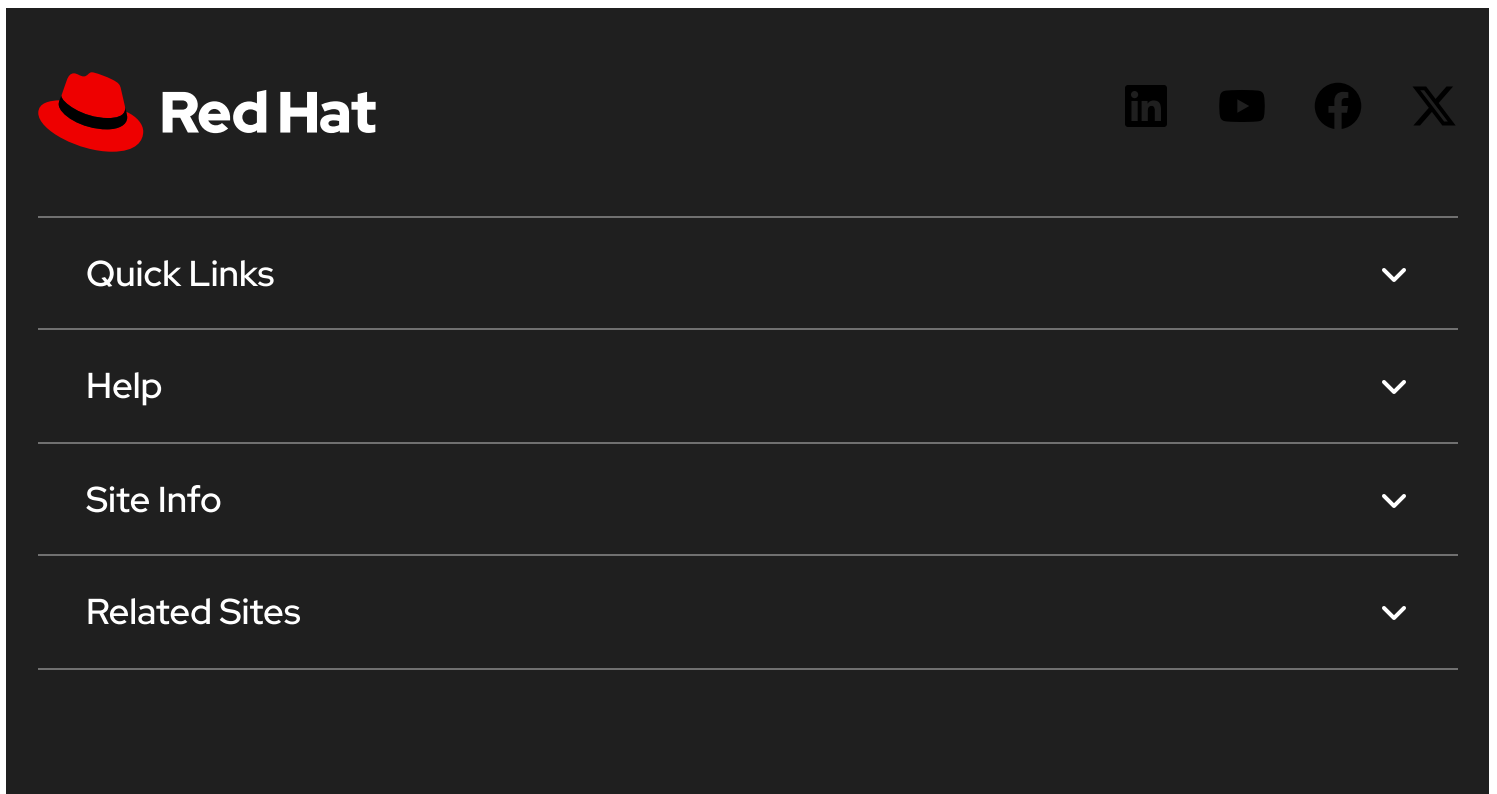
- CVE-2025-4953 [↗](#)

- [CVE-2025-11561](#)
- [CVE-2025-31133](#)
- [CVE-2025-52565](#)
- [CVE-2025-52881](#)


## References


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

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, which consists of a red fedora hat icon followed by the text "Red Hat" in white. On the right side of the bar are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the bar is a vertical menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item is followed by a white downward-pointing chevron icon, indicating that these are expandable sections.

 All systems operational



The image shows a dark-themed footer navigation menu. It starts with a small, light-colored icon of a fedora hat. Below the icon are four text links: "About Red Hat", "Jobs", "Events", and "Locations", all in a light gray color.

[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](#)