

[Red Hat Product Errata](#)    [RHSA-2026:0332 - Security Advisory](#)

# RHSA-2026:0332 - Security Advisory

Issued: 2026-01-15

Updated: 2026-01-15

[Overview](#)

## Synopsis

Important: OpenShift Container Platform 4.18.31 bug fix and security update

## Type/Severity

Security Advisory: Important

## Topic

Red Hat OpenShift Container Platform release 4.18.31 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 4.18.

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

<https://access.redhat.com/errata/RHSA-2026:0331> 

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/4.18/html/release\\_notes/](https://docs.redhat.com/en/documentation/openshift_container_platform/4.18/html/release_notes/) 

#### Security Fix(es):

- bind: Resource exhaustion via malformed DNSKEY handling (CVE-2025-8677)
- bind: Cache poisoning attacks with unsolicited RRs (CVE-2025-40778)
- bind: Cache poisoning due to weak PRNG (CVE-2025-40780)
- expat: libexpat in Expat allows attackers to trigger large dynamic memory


allocations via a small document that is submitted for parsing (CVE-2025-59375)

- openssl: Out-of-bounds read & write in RFC 3211 KEK Unwrap

(CVE-2025-9230)

- qemu-kvm: VNC WebSocket handshake use-after-free (CVE-2025-11234)

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 4.18 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/4.18/html-single/updating\\_clusters/index#updating-cluster-cli](https://docs.redhat.com/en/documentation/openshift_container_platform/4.18/html-single/updating_clusters/index#updating-cluster-cli). 

## Solution

For OpenShift Container Platform 4.18 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/4.18/html/release\\_notes/](https://docs.redhat.com/en/documentation/openshift_container_platform/4.18/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

sha256:64e8c4cbd3199beb1ebb8d6a208cb81fdfe62f4e52d7586033f534d35f981244

(For s390x architecture)

The image digest is

sha256:5b964fa43873a20a66b95769bbcd6c31b028f505281fb045bb3c2ed6ca114e91

(For ppc64le architecture)

The image digest is

sha256:2108325c5ee08249e1b0c0ad6a3daab197f5e2a1a83c8600d27c49ad0ff94307

(For aarch64 architecture)

The image digest is

sha256:b465cef295a81eaf055c87a9af6d8ecdcc11cb1e898895d6df527eb155a7ff82

All OpenShift Container Platform 4.18 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/4.18/html-single/updating\\_clusters/index#updating-cluster-cli](https://docs.redhat.com/en/documentation/openshift_container_platform/4.18/html-single/updating_clusters/index#updating-cluster-cli). ↗

## Affected Products

- Red Hat OpenShift Container Platform 4.18 for RHEL 9 x86\_64
- Red Hat OpenShift Container Platform 4.18 for RHEL 8 x86\_64
- Red Hat OpenShift Container Platform for Power 4.18 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.18 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.18 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.18 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.18 for RHEL 9 aarch64

- Red Hat OpenShift Container Platform for ARM 64 4.18 for RHEL 8 aarch64

## Fixes

- BZ - 2395108 [↗](#) - CVE-2025-59375 expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing
- BZ - 2396054 [↗](#) - CVE-2025-9230 openssl: Out-of-bounds read & write in RFC 3211 KEK Unwrap
- BZ - 2401209 [↗](#) - CVE-2025-11234 qemu-kvm: VNC WebSocket handshake use-after-free
- BZ - 2405827 [↗](#) - CVE-2025-40778 bind: Cache poisoning attacks with unsolicited RRs
- BZ - 2405829 [↗](#) - CVE-2025-40780 bind: Cache poisoning due to weak PRNG
- BZ - 2405830 [↗](#) - CVE-2025-8677 bind: Resource exhaustion via malformed DNSKEY handling
- OCPBUGS-64613 [↗](#) - [4.18] coreos-boot-disk link not working with multipath on early boot

## CVEs

- CVE-2025-8677 [↗](#)
- CVE-2025-9230 [↗](#)
- CVE-2025-11234 [↗](#)
- CVE-2025-40778 [↗](#)
- CVE-2025-40780 [↗](#)
- CVE-2025-59375 [↗](#)

## 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/>.



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](#)