



RHSA-2025:4211 - Security Advisory

Issued: 2025-05-01 Updated: 2025-05-01

[Overview](#)[Updated Images](#)

Synopsis

Important: OpenShift Container Platform 4.18.11 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.18.11 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 4.18.11. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHBA-2025:4213> [↗](#)

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/
✍

Security Fix(es):

- golang-jwt/jwt: jwt-go allows excessive memory allocation during header

parsing (CVE-2025-30204)

- cri-o: Checkpoint restore can be triggered from different namespaces

(CVE-2024-8676)

- go-jose: Go JOSE's Parsing Vulnerable to Denial of Service

(CVE-2025-27144)

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. ✍

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/
✍

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:b3c76706606940d84964095aaab1a8ed4eca0d1bd6833b4eb718115842ef6850

(For s390x architecture)

The image digest is

sha256:ba245bfdba7d81161971640e255f334e20b281ef15342dbf2587504bd30d3a94

(For ppc64le architecture)

The image digest is

sha256:749484f20536a9a75ce57e4fafd57f6216e596256ed2f712a769ebb3e7c785f4

(For aarch64 architecture)

The image digest is

sha256:b5c055b54ca8581f11a3acfd72bcace0319f6f9aca35f834996fa579b6543dd9













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. ↗

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 - 2313842](#) ↗ - CVE-2024-8676 cri-o: Checkpoint restore can be triggered from different namespaces
- [BZ - 2347423](#) ↗ - CVE-2025-27144 go-jose: Go JOSE's Parsing Vulnerable to Denial of Service
- [BZ - 2354195](#) ↗ - CVE-2025-30204 golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing
- [OCPBUGS-36610](#) ↗ - periodic-ci-openshift-appliance-master-e2e-sno-dualstack-dhcp-periodic not cleaning up after itself

- [OCPBUGS-39305](#)  - APIRequestCount should not record violations for APIs that are not served
- [OCPBUGS-53278](#)  - In OCL. Cannot install extensions
- [OCPBUGS-54369](#)  - Can't use WWN to select between multipath disks
- [OCPBUGS-54594](#)  - RHEL 8 aleph aarch64 RHCOS will fail to boot 4.19 (RHEL 9.6) without bootloader update
- [OCPBUGS-54698](#)  - CNO Missing servicemonitors and prometheusrules permissions for non-OVN Kubernetes
- [OCPBUGS-54817](#)  - mtu-migration service fails with NMState br-ex
- [OCPBUGS-54947](#)  - OpenShift 4.17 IPI Private cluster installation failure due to static IP not in range of Subnet
- [OCPBUGS-55116](#)  - Revert "Add delay in linuxptp-daemon to wait for socket to be ready"
- [OCPBUGS-55146](#)  - Use 135 for terminationGracePeriodSeconds for v2 KAS
- [OCPBUGS-55172](#)  - OLMv1: Component Readiness: [Unknown] [Other] test regressed: n=2 x509 error
- [OCPBUGS-55240](#)  - Upgrading from 4.16 to 4.17 causes the Cluster Resource Override Operator to stop working
- [OCPBUGS-55242](#)  - The apiservice v1.admission.autoscaling.openshift.io gets not reachable after deleting the ClusterResourceOverride for clusterresourceoverride-operator

CVEs

- [CVE-2024-8676](#) 
- [CVE-2025-27144](#) 
- [CVE-2025-30204](#) 

References

- <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/>.



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](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)