



Red Hat Product Errata RHSA-2025:3577 - Security Advisory

RHSA-2025:3577 - Security Advisory

Issued: 2025-04-10 Updated: 2025-04-10

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

Synopsis

Important: OpenShift Container Platform 4.18.8 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.18.8 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 4.18.8. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHBA-2025:3579> 

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):

- podman: buildah: Container breakout by using `--jobs=2` and a race

condition when building a malicious Containerfile (CVE-2024-11218)


- grub2: net: Out-of-bounds write in `grub_net_search_config_file()`

(CVE-2025-0624)

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

parsing (CVE-2025-30204)


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

sha256:509888097ba7d3b4eeb5aac0586acff2ec13fff07004ac692e0dcf5cf4fe2690

(For s390x architecture)

The image digest is

sha256:7af6036c5d10145fa4d4138aeeb07ac812f658b100913cf8722f365973566b1e

(For ppc64le architecture)


The image digest is

sha256:c36276a6a0473f03319fb57179538a41ca9e75c1c30d0a5e5a277a082135d6e9

(For aarch64 architecture)

The image digest is






sha256:b9dd5873644fcab301178105df2b45e29d885da98b373a215329b610efb6c6ec

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 - 2326231](#)  - CVE-2024-11218 podman: buildah: Container breakout by using --jobs=2 and a race condition when building a malicious Containerfile
- [BZ - 2346112](#)  - CVE-2025-0624 grub2: net: Out-of-bounds write in grub_net_search_config_file()
- [BZ - 2354195](#)  - CVE-2025-30204 golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing
- [OCPBUGS-44769](#)  - [GCP-PD] Hyperdisk does not support rwx
- [OCPBUGS-52494](#)  - GCP MAPI seemingly reconciles MachineSet with incompatible shieldedInstanceConfig

- [OCPBUGS-52496](#) - Component Readiness: [Cloud Compute / Unknown] [Other] test regressed
- [OCPBUGS-52949](#) - [release-4.18] Unexpected Behavior During Cluster Upgrade (4.14.23 to 4.15.15) for the ovn-ipsec-host pods.
- [OCPBUGS-53080](#) - [4.18] Add missing relatedObjects to CBO
- [OCPBUGS-53345](#) - SNYK: Medium severity vulnerability found in github.com/golang/glog
- [OCPBUGS-53371](#) - Increasing Clock Class Reporting Frequency
- [OCPBUGS-53388](#) - Missing version values for oc-mirror --v2
- [OCPBUGS-53453](#) - [IBMCloud] the CIS "plugin did not respond" blocked the public install
- [OCPBUGS-54205](#) - [v2] oc-mirror delete plugin --help syntax error
- [OCPBUGS-54269](#) - [release-4.18] /k8s/all-namespaces/volumesnapshots returns 404 Page Not Found
- [OCPBUGS-54355](#) - Add status check for Azure NIC provisioning
- [OCPBUGS-54462](#) - OSUpdateStarted event should only be emitted on actual OS updates

CVEs

- [CVE-2023-52653](#)
- [CVE-2024-2236](#)
- [CVE-2024-11218](#)
- [CVE-2024-23848](#)
- [CVE-2024-26976](#)
- [CVE-2024-27010](#)
- [CVE-2024-27410](#)
- [CVE-2024-35810](#)
- [CVE-2024-35888](#)
- [CVE-2024-35925](#)
- [CVE-2024-50264](#)
- [CVE-2025-0624](#)
- [CVE-2025-22013](#)
- [CVE-2025-24855](#)
- [CVE-2025-27363](#)
- [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



✔ 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