



# Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

**RHSA**

25-11-13

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

**Synop**

Importa

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

**Type/**

Security

**Topic**

Red Hat  
images t

**Accept default** will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

ages and

This rele

**Required Cookies only** will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Common  
ailable

**Descri**

Red Hat  
platform

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy

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/4.12/html/release\\_notes](https://docs.redhat.com/en/documentation/openshift_container_platform/4.12/html/release_notes)



## Security Fix(es):

None


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 4.12 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/4.12/html-single/updating\\_clusters/index#updating-cluster-within-minor](https://docs.redhat.com/en/documentation/openshift_container_platform/4.12/html-single/updating_clusters/index#updating-cluster-within-minor). 

## Solution

For OpenShift Container Platform 4.12 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/4.12/html/release\\_notes](https://docs.redhat.com/en/documentation/openshift_container_platform/4.12/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 value for the release is as follows:

(For x86\_64 architecture)

The image digest is

sha256:d26fd3fd30ac6ae13f2779045d4e2defbf77aa24db5393d91df19488fd42504d

All OpenShift Container Platform 4.12 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/4.12/html-single/updating\\_clusters/index#updating-cluster-within-minor](https://docs.redhat.com/en/documentation/openshift_container_platform/4.12/html-single/updating_clusters/index#updating-cluster-within-minor). 

## Affected Products

- Red Hat OpenShift Container Platform 4.12 for RHEL 9 x86\_64
- Red Hat OpenShift Container Platform 4.12 for RHEL 8 x86\_64
- Red Hat OpenShift Container Platform for Power 4.12 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.12 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 for RHEL 9 s390x

- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.12 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.12 for RHEL 8 aarch64

## Fixes

- [BZ - 2372373](#) [↗](#) - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- [BZ - 2372385](#) [↗](#) - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- [BZ - 2380149](#) [↗](#) - CVE-2025-6965 sqlite: Integer Truncation in SQLite
- [BZ - 2380949](#) [↗](#) - CVE-2025-5994 unbound: Unbound Cache poisoning
- [BZ - 2392595](#) [↗](#) - CVE-2025-58060 cups: Authentication Bypass in CUPS Authorization Handling
- [BZ - 2393152](#) [↗](#) - CVE-2025-9566 podman: Podman kube play command may overwrite host files

## CVEs

- [CVE-2025-5994](#) [↗](#)
- [CVE-2025-6965](#) [↗](#)
- [CVE-2025-9566](#) [↗](#)
- [CVE-2025-49794](#) [↗](#)
- [CVE-2025-49796](#) [↗](#)
- [CVE-2025-58060](#) [↗](#)

## 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



 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 and Opt-Out Rights](#)