RHSA-2026:0677 - Security Advisory

Issued: 2026-01-22 Updated: 2026-01-22

Overview

Synopsis

Important: OpenShift Container Platform 4.13.63 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.13.63 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 4.13.

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

https://access.redhat.com/errata/RHSA-2026:0676

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/4.13/html/release_notes

Security Fix(es):

- libxslt: libxml2: Inifinite recursion at exsltDynMapFunction function in libexslt/dynamic.c (CVE-2025-9714)
- expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing (CVE-2025-59375)
- sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems (CVE-2025-11561)
- bind: Cache poisoning attacks with unsolicited RRs (CVE-2025-40778)
- bind: Cache poisoning due to weak PRNG (CVE-2025-40780)
- bind: Resource exhaustion via malformed DNSKEY handling (CVE-2025-8677)

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 4.13 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/4.13/html-single/updating_clusters/index#updating-cluster-within-minor.

Solution

For OpenShift Container Platform 4.13 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/4.13/html/release_notes

You may download the oc tool and use it to inspect release image metadata for x86_64 architecture. The image digest 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:b373f9055bf22079e7baf0c7b3ea21067248932bb0ec57fa0af30c51810bbe91

All OpenShift Container Platform 4.13 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/4.13/html-single/updating_clusters/index#updating-cluster-within-minor.

Affected Products

- Red Hat OpenShift Container Platform 4.13 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.13 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 8 aarch64

Fixes

- BZ - 2392605 - CVE-2025-9714 libxslt: libxml2: Inifinite recursion at exsltDynMapFunction function in libexslt/dynamic.c
- 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 - 2402727 - CVE-2025-11561 sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems
- 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

CVEs

- CVE-2025-8677
- CVE-2025-9714
- CVE-2025-11561
- CVE-2025-40778
- CVE-2025-40780
- CVE-2025-59375

References

- https://access.redhat.com/security/updates/classification/#important
- https://docs.redhat.com/en/documentation/openshift_container_platform/4.13/html/release_notes

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.

Red Hat

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie Preferences and Opt-Out Rights