RHSA-2026:0702 - Security Advisory

发布： 2026-01-22 已更新： 2026-01-22

概述

概述

Important: OpenShift Container Platform 4.17.47 bug fix and security update

类型/严重性

Security Advisory: Important

标题

Red Hat OpenShift Container Platform release 4.17.47 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 4.17.

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.

描述

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

https://access.redhat.com/errata/RHSA-2026:0701

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/4.17/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)

- libssh: Invalid return code for chacha20 poly1305 with OpenSSL backend

(CVE-2025-5987)

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

(CVE-2025-9230)

- libxslt: libxml2: Inifinite recursion at exsltDynMapFunction function in

libexslt/dynamic.c (CVE-2025-9714)

- 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 4.17 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/4.17/html-single/updating_clusters/index#updating-cluster-cli.

解决方案

For OpenShift Container Platform 4.17 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/4.17/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:d49a4f1a4532e3822e8769a97d87f538f9101701d3997e6e883c8abff7b58a43

(For s390x architecture)
The image digest is sha256:baded7c05358eda3d7bc20efdc3d2b963ba80f1639c2c80b2c58bc216a1375d1

(For ppc64le architecture)
The image digest is sha256:4714f7f59793e8f77cc5a95eb918bd43f9a6ff31de1b35fb59b45a07f7a3f118

(For aarch64 architecture)
The image digest is sha256:73e2429c13a91ea4e5031c61f94c57884a7251ece3e1bbb338523e7bf8246903

All OpenShift Container Platform 4.17 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/4.17/html-single/updating_clusters/index#updating-cluster-cli.

受影响的产品

- Red Hat OpenShift Container Platform 4.17 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.17 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.17 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.17 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 8 aarch64

修复

- BZ - 2376219 - CVE-2025-5987 libssh: Invalid return code for chacha20 poly1305 with OpenSSL backend
- 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 - 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

CVE

- CVE-2025-5987
- CVE-2025-8677
- CVE-2025-9230
- CVE-2025-9714
- CVE-2025-11234
- CVE-2025-40778
- CVE-2025-40780
- CVE-2025-59375

参考

- https://access.redhat.com/security/updates/classification/#important

Red Hat 安全团队联络方式为 secalert@redhat.com。 更多联络细节请参考 https://access.redhat.com/security/team/contact/。