RHSA-2025:1123 - Security Advisory

Issued: 2025-02-12 Updated: 2025-02-12

Synopsis

Important: OpenShift Container Platform 4.16.34 security and extras update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.16.34 is now available with updates to packages and images that fix several bugs.

This release includes a security update for Red Hat OpenShift Container Platform 4.16.

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 RPM packages for Red Hat OpenShift Container Platform 4.16.34. See the following advisory for the container images for this release:

https://access.redhat.com/errata/RHBA-2025:1124

Security Fix(es):

- golang.org/x/net/html: Non-linear parsing of case-insensitive content in

golang.org/x/net/html (CVE-2024-45338)

- jinja2: Jinja has a sandbox breakout through malicious filenames

(CVE-2024-56201)

- jinja2: Jinja has a sandbox breakout through indirect reference to format

method (CVE-2024-56326)

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 4.16 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.openshift.com/container-platform/4.16/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.16 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.openshift.com/container-platform/4.16/release_notes/ocp-4-16-release-notes.html

Affected Products

- Red Hat OpenShift Container Platform 4.16 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 9 aarch64

Fixes

- BZ - 2330539 - CVE-2024-12085 rsync: Info Leak via Uninitialized Stack Contents
- BZ - 2333122 - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- BZ - 2333854 - CVE-2024-56201 jinja2: Jinja has a sandbox breakout through malicious filenames

- BZ - 2333856 - CVE-2024-56326 jinja2: Jinja has a sandbox breakout through indirect reference to format method

CVEs

- CVE-2024-12085
- CVE-2024-45338
- CVE-2024-56201
- CVE-2024-56326

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/.