RHSA-2024:0045 - Security Advisory

Issued: 2024-06-27 Updated: 2024-06-27

Synopsis

Important: OpenShift Container Platform 4.16.0 security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

Red Hat OpenShift Container Platform release 4.16.0 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 4.16.

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 4.16.0. See the following advisory for the container images for this release:

https://access.redhat.com/errata/RHSA-2024:0041

Security Fix(es):

- dnspython: denial of service in stub resolver (CVE-2023-29483)
- golang: net/http/cookiejar: incorrect forwarding of sensitive headers and

cookies on HTTP redirect (CVE-2023-45289)

- golang: net/http: memory exhaustion in Request.ParseMultipartForm

(CVE-2023-45290)

- containers/image: digest type does not guarantee valid type

(CVE-2024-3727)

- golang: crypto/x509: Verify panics on certificates with an unknown public

key algorithm (CVE-2024-24783)

- golang: net/mail: comments in display names are incorrectly handled

(CVE-2024-24784)

- golang: html/template: errors returned from MarshalJSON methods may break

template escaping (CVE-2024-24785)

- golang-protobuf: encoding/protojson, internal/encoding/json: infinite

loop in protojson.Unmarshal when unmarshaling certain forms of invalid JSON (CVE-2024-24786)

- jose: resource exhaustion (CVE-2024-28176)

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 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

Affected Products

- Red Hat OpenShift Container Platform 4.16 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.16 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 8 aarch64

Fixes

- BZ - 2262921 - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads

- BZ - 2268017 - CVE-2023-45290 golang: net/http: memory exhaustion in Request.ParseMultipartForm
- BZ - 2268018 - CVE-2023-45289 golang: net/http/cookiejar: incorrect forwarding of sensitive headers and cookies on HTTP redirect
- BZ - 2268019 - CVE-2024-24783 golang: crypto/x509: Verify panics on certificates with an unknown public key algorithm
- BZ - 2268021 - CVE-2024-24784 golang: net/mail: comments in display names are incorrectly handled
- BZ - 2268022 - CVE-2024-24785 golang: html/template: errors returned from MarshalJSON methods may break template escaping
- BZ - 2268046 - CVE-2024-24786 golang-protobuf: encoding/protojson, internal/encoding/json: infinite loop in protojson.Unmarshal when unmarshaling certain forms of invalid JSON
- BZ - 2268820 - CVE-2024-28176 jose: resource exhaustion
- BZ - 2274520 - CVE-2023-29483 dnspython: denial of service in stub resolver
- BZ - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type

CVEs

- CVE-2023-29483
- CVE-2023-45289
- CVE-2023-45290
- CVE-2024-3727
- CVE-2024-24783
- CVE-2024-24784
- CVE-2024-24785
- CVE-2024-24786
- CVE-2024-28176

References

- https://access.redhat.com/security/updates/classification/#important
- https://docs.openshift.com/container-platform/4.16/release_notes/ocp-4-16-release-notes.html

---

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

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility