Red Hat F

RHSA

Advis

Overview

Updated P

4-08-13

Synop

Importa

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update for the container-tools:rhel8 module is now available for Red Hat Enterprise Linux 8.

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

The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.

Security Fix(es):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)
- golang: net/http: memory exhaustion in Request.ParseMultipartForm (CVE-2023-45290)
- 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)
- containers/image: digest type does not guarantee valid type (CVE-2024-3727)
- golang: archive/zip: Incorrect handling of certain ZIP files (CVE-2024-24789)
- go-retryablehttp: url might write sensitive information to log file (CVE-2024-6104)
- gorilla/schema: Potential memory exhaustion attack due to sparse slice deserialization (CVE-2024-37298)

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.

Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

Affected Products

- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

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 - 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 - 2274767 - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2292668 - CVE-2024-24789 golang: archive/zip: Incorrect handling of certain ZIP files
- BZ - 2294000 - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- BZ - 2295010 - CVE-2024-37298 gorilla/schema: Potential memory exhaustion attack due to sparse slice deserialization
- RHEL-40801 - Listing tags in JFrog Artifactory may fail - Skopeo RHEL 8.10
- RHEL-40800 - Listing tags in JFrog Artifactory may fail - Podman RHEL 8.10

CVEs

- CVE-2023-45290
- CVE-2024-1394
- CVE-2024-3727
- CVE-2024-6104
- CVE-2024-24783
- CVE-2024-24784
- CVE-2024-24789
- CVE-2024-37298
- CVE-2024-37891

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/.

Quick Links

Help

Site Info

Related Sites

Loading