RHSA-2024:5634 - Security Advisory

Issued: 2024-08-20 Updated: 2024-08-20

Synopsis

Important: podman security update

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 podman is now available for Red Hat Enterprise Linux 9.2 Extended Update Support.

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 podman tool manages pods, container images, and containers. It is part of the libpod library, which is for applications that use container pods. Container pods is a concept in Kubernetes.

Security Fix(es):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)
- 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 - Extended Update Support 9.2 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x

Fixes

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

- 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

CVEs

- CVE-2024-1394
- CVE-2024-6104
- CVE-2024-37298

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/.