RHSA-2024:4379 - Security Advisory

Issued: 2024-07-08 Updated: 2024-07-08

Synopsis

Important: gvisor-tap-vsock 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 gvisor-tap-vsock is now available for Red Hat Enterprise Linux 9.

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

A replacement for libslirp and VPNKit, written in pure Go. It is based on the network stack of gVisor and is used to provide networking for podman-machine virtual machines. Compared to libslirp, gvisor-tap-vsock brings a configurable DNS server and dynamic port forwarding.

Security Fix(es):

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

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 9 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64

- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x

Fixes

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

CVEs

- CVE-2024-1394

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/.