RHSA-2024:9136 - Security Advisory

Issued: 2024-11-12 Updated: 2024-11-12

Synopsis

Moderate: qemu-kvm security update

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update for qemu-kvm is now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm packages provide the user-space component for running virtual machines that use KVM.

Security Fix(es):

- QEMU: SR-IOV: improper validation of NumVFs leads to buffer overflow (CVE-2024-26327)
- QEMU: virtio: DMA reentrancy issue leads to double free vulnerability (CVE-2024-3446)
- QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure (CVE-2024-7409)

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.

Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 9.5 Release Notes linked from 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 Server - AUS 9.6 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 Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 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 Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x

Fixes

- BZ - 2264844 - CVE-2024-26327 QEMU: SR-IOV: improper validation of NumVFs leads to buffer overflow
- BZ - 2274211 - CVE-2024-3446 QEMU: virtio: DMA reentrancy issue leads to double free vulnerability

- BZ - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- RHEL-17719 - allow keeping 'raw' in 'backing field format' when the 'raw' driver layer will be dropped
- RHEL-21695 - [Qemu] Improve the tracing output of qemu tools(qemu-img/qemu-io)
- RHEL-24024 - Qemu core dump when do zero copy through exec
- RHEL-28073 - Rebase qemu-kvm to QEMU 9.0.0 for RHEL 9.5
- RHEL-28813 - qemu crash with kvm_irqchip_commit_routes: Assertion `ret == 0' failed if booting with many virtio disks and vcpus
- RHEL-30362 - Check/fix machine type compatibility for QEMU 9.0.0 [x86_64][rhel-9.5.0]
- RHEL-33889 - Support zero-page-detection for multifd from qemu-kvm-9.0.0
- RHEL-34945 - [aarch64, kvm-unit-tests] all tests tagged as FAIL [qemu-kvm: GLib: g_ptr_array_add: assertion 'rarray' failed]
- RHEL-33440 - Qemu hang when quit dst vm after storage migration(nbd+tls)
- RHEL-34621 - [RHEL9.5.0][stable_guest_abi]Failed to migrate VM with (qemu) qemu-kvm: Missing section footer for 0000:00:01.0/virtio-gpu qemu-kvm: load of migration failed: Invalid argument
- RHEL-34618 - aio=io_uring: Assertion failure `luringcb->co->ctx == s->aio_context' with block_resize
- RHEL-36159 - qemu crash on Assertion `block->n_free_ciphers > 0' failed in guest installation with luks and iothread-vq-mapping [rhel-9.5]
- RHEL-38697 - aio=native: Assertion failure `laiocb->co->ctx == laiocb->ctx->aio_context' with block_resize
- RHEL-42411 - qemu-kvm: linux-aio: add support for IO_CMD_FDSYNC command
- RHEL-28686 - Rebuild qemu-kvm with clang 18 [rhel-9]
- RHEL-40708 - [RHEL9.5.0][virtio_fs][s390x] after hot-unplug the vhost-user-fs-ccw device, the device is failed to hot-plug again
- RHEL-50000 - scsi-block: Cannot setup Windows Failover Cluster, qemu crashes on assert [rhel-9.5]

CVEs

- CVE-2024-3446
- CVE-2024-7409
- CVE-2024-26327

References

- https://access.redhat.com/security/updates/classification/#moderate
- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/9.5_release_notes/index

---

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