RHSA-2019:2553 - Security Advisory

Issued: 2019-08-22 Updated: 2019-08-22

Synopsis

Important: qemu-kvm-rhev security, bug fix, and enhancement 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 qemu-kvm-rhev is now available for Red Hat Virtualization 4 for Red Hat Enterprise Linux 7 and Red Hat Virtualization Engine 4.3.

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

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

Security Fix(es):

- A flaw was found in the implementation of the "fill buffer", a mechanism used by modern CPUs when a cache-miss is made on L1 CPU cache. If an attacker can generate a load operation that would create a page fault, the execution will continue speculatively with incorrect data from the fill buffer while the data is fetched from higher level caches. This response time can be measured to infer data in the fill buffer. (CVE-2018-12130)
- Modern Intel microprocessors implement hardware-level micro-optimizations to improve the performance of writing data back to CPU caches. The write operation is split into STA (STore Address) and STD (STore Data) sub-operations. These sub-operations allow the processor to hand-off address generation logic into these sub-operations for optimized writes. Both of these sub-operations write to a shared distributed processor structure called the 'processor store buffer'. As a result, an unprivileged attacker could use this flaw to read private data resident within the CPU's processor store buffer. (CVE-2018-12126)
- Microprocessors use a ‘load port’ subcomponent to perform load operations from memory or IO. During a load operation, the load port receives data from the memory or IO subsystem and then provides the data to the CPU registers and operations in the CPU’s pipelines. Stale load operations results are stored in the 'load port' table until overwritten by newer operations. Certain load-port operations triggered by an attacker can be used to reveal data about previous stale requests leaking data back to the attacker via a timing side-channel. (CVE-2018-12127)
- Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. (CVE-2019-11091)
- QEMU: device_tree: heap buffer overflow while loading device tree blob (CVE-2018-20815)
- QEMU: rtl8139: integer overflow leads to buffer overflow (CVE-2018-17958)
- QEMU: net: ignore packets with large size (CVE-2018-17963)
- QEMU: scsi-generic: possible OOB access while handling inquiry request (CVE-2019-6501)
- QEMU: slirp: information leakage in tcp_emu() due to uninitialized stack variables (CVE-2019-9824)

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:

This update also fixes several bugs and adds various enhancements. Documentation for these changes is available from the Release Notes document linked to 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/2974891

After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

Affected Products

- Red Hat Virtualization Manager 4.3 x86_64
- Red Hat Virtualization 4 for RHEL 7 x86_64
- Red Hat Virtualization for IBM Power LE 4 for RHEL 7 ppc64le

Fixes

- BZ - 1508708 - [data plane] Qemu-kvm core dumped when doing block-stream and block-job-cancel to a data disk with data-plane enabled
- BZ - 1526313 - Improve QEMU lock error info for hot-plugging same qcow2 image file twice in different target to VM
- BZ - 1531888 - Local VM and migrated VM on the same host can run with same RAW file as visual disk source while without shareable configured or lock manager enabled
- BZ - 1551486 - QEMU image locking needn't double open fd number (i.e. drop file-posix.c:s->lock_fd)
- BZ - 1585155 - QEMU core dumped when hotplug memory exceeding host hugepages and with discard-data=yes
- BZ - 1597482 - qemu crashed when disk enable the IOMMU
- BZ - 1598119 - "share-rw=on" does not work for luks format image
- BZ - 1603104 - Qemu Aborted (core dumped) for 'qemu-kvm: Failed to lock byte 100' when remote NFS or GlusterFS volume stopped during the block mirror(or block commit/stream) process
- BZ - 1607768 - qemu aborted when start guest with a big iothreads
- BZ - 1608226 - [virtual-network][mq] prompt warning "qemu-kvm: unable to start vhost net: 14: falling back on userspace virtio" when boot with win8+ guests with multi-queue
- BZ - 1610461 - High Host CPU load for Windows 10 Guests (Update 1803) when idle
- BZ - 1614302 - qemu-kvm: Could not find keytab file: /etc/qemu/krb5.tab: No such file or directory
- BZ - 1614610 - Guest quit with error when hotunplug cpu
- BZ - 1619778 - Ballooning is incompatible with vfio assigned devices, but not prevented

- BZ - 1620373 - Failed to do migration after hotplug and hotunplug the ivshmem device
- BZ - 1623986 - block-commit can't be used with -blockdev
- BZ - 1624009 - allow backing of pflash via -blockdev
- BZ - 1627272 - boot guest with q35+vIOMMU+ device assignment, qemu crash when return assigned network devices from vfio driver to ixgbe in guest
- BZ - 1628098 - [Intel 7.7 BUG][KVM][Crystal Ridge]object_get_canonical_path_component: assertion failed: (obj->parent != NULL)
- BZ - 1629056 - qemu NBD server failure with block status of dirty bitmaps
- BZ - 1629717 - qemu_ram_mmap: Assertion `is_power_of_2(align)' failed
- BZ - 1629720 - [Intel 7.6 BUG][Crystal Ridge] pc_dimm_get_free_addr: assertion failed: (QEMU_ALIGN_UP(address_space_start, align) == address_space_start)
- BZ - 1631052 - x-block-dirty-bitmap-merge into a disabled bitmap dest causes assert
- BZ - 1631227 - Qemu Core dump when quit vm that's in status "paused(io-error)" with data plane enabled
- BZ - 1631615 - Wrong werror default for -device drive=<node-name>
- BZ - 1631877 - qemu dirty bitmap merge fails to update count
- BZ - 1633150 - Cross migration from RHEL7.5 to RHEL7.6 fails with cpu flag stibp
- BZ - 1633536 - Qemu core dump when do migration after hot plugging a backend image with 'blockdev-add'(without the frontend)
- BZ - 1636712 - CVE-2018-17958 QEMU: rtl8139: integer overflow leads to buffer overflow
- BZ - 1636777 - CVE-2018-17963 QEMU: net: ignore packets with large size
- BZ - 1642551 - qemu-kvm-tools-rhev depends on libxkbcommon, but the RPM-level dependency is missing
- BZ - 1646781 - CVE-2018-12126 hardware: Microarchitectural Store Buffer Data Sampling (MSBDS)
- BZ - 1646784 - CVE-2018-12130 hardware: Microarchitectural Fill Buffer Data Sampling (MFBDS)
- BZ - 1648236 - QEMU doesn't expose rendernode option for egl-headless display type
- BZ - 1656913 - qcow2 cache is too small
- BZ - 1666336 - severe performance impact using encrypted Cinder volume (QEMU luks)
- BZ - 1666884 - persistent bitmaps prevent qcow2 image resize
- BZ - 1667320 - -blockdev: auto-read-only is ineffective for drivers on read-only whitelist
- BZ - 1667782 - CVE-2018-12127 hardware: Micro-architectural Load Port Data Sampling - Information Leak (MLPDS)
- BZ - 1668160 - CVE-2019-6501 QEMU: scsi-generic: possible OOB access while handling inquiry request
- BZ - 1668956 - incremental backup bitmap API needs a finalized interface
- BZ - 1672010 - [RHEL7]Qemu coredump when remove a persistent bitmap after vm re-start(dataplane enabled)

- BZ - 1673080 - "An unknown error has occurred" when using cdrom to install the system with two blockdev disks.(when choose installation destination)
- BZ - 1673397 - [RHEL.7] qemu-kvm core dumped after hotplug the deleted disk with iothread parameter
- BZ - 1673402 - Qemu core dump when start guest with two disks using same drive
- BZ - 1676728 - RHEL77: Run iotests as part of build process
- BZ - 1677073 - Backport additional QEMU 4.0 Bitmap API changes to RHEL 7.7
- BZ - 1678515 - CVE-2019-9824 QEMU: slirp: information leakage in tcp_emu() due to uninitialized stack variables
- BZ - 1685989 - Add facility to use block jobs with backing images without write permission
- BZ - 1691009 - NBD pull mode incremental backup API needs a finalized interface
- BZ - 1691018 - Fix iotest 226 for local development builds
- BZ - 1691048 - Add qemu-img info support for querying bitmaps offline
- BZ - 1691563 - QEMU NBD Feature parity roundup (QEMU 3.1.0)
- BZ - 1692018 - qemu-img: Protocol error: simple reply when structured reply chunk was expected
- BZ - 1693101 - CVE-2018-20815 QEMU: device_tree: heap buffer overflow while loading device tree blob
- BZ - 1703916 - Qemu core dump when quit vm after forbidden to do backup with a read-only bitmap
- BZ - 1705312 - CVE-2019-11091 hardware: Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
- BZ - 1714160 - Guest with 'reservations' for a disk start failed

CVEs

- CVE-2018-12126
- CVE-2018-12127
- CVE-2018-12130
- CVE-2018-17958
- CVE-2018-17963
- CVE-2018-20815
- CVE-2019-6501
- CVE-2019-9824
- CVE-2019-11091

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/security/vulnerabilities/mds

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.