Red Hat F

RHSA
Advis

-08-09

Overview

Updated P

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 qemu-kvm-rhev is now available for Red Hat OpenStack Platform 10.0 (Newton), Red Hat OpenStack Platform 13.0 (Queens), and Red Hat OpenStack Platform 14.0 (Rocky).

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):

- QEMU: slirp: heap buffer overflow in tcp_emu() (CVE-2019-6778)
- QEMU: rtl8139: integer overflow leads to buffer overflow (CVE-2018-17958)
- QEMU: net: ignore packets with large size (CVE-2018-17963)
- QEMU: seccomp: blacklist is not applied to all threads (CVE-2018-15746)
- 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.

Bug Fix(es):

- Update qemu-kvm-rhev for RHEL 7.7 compatibility [OSP-14] (BZ#1728358)
- Update qemu-kvm-rhev for RHEL 7.7 compatibility [OSP-13] (BZ#1728359)
- Update qemu-kvm-rhev for RHEL 7.7 compatibility [OSP-10] (BZ#1728360)

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

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 OpenStack for IBM Power 14 ppc64le
- Red Hat OpenStack for IBM Power 13 ppc64le
- Red Hat OpenStack 14 x86_64
- Red Hat OpenStack 13 x86_64
- Red Hat OpenStack 10 x86_64

Fixes

- BZ - 1615637 - CVE-2018-15746 QEMU: seccomp: blacklist is not applied to all threads
- 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 - 1664205 - CVE-2019-6778 QEMU: slirp: heap buffer overflow in tcp_emu()
- BZ - 1668160 - CVE-2019-6501 QEMU: scsi-generic: possible OOB access while handling inquiry request
- BZ - 1678515 - CVE-2019-9824 QEMU: slirp: information leakage in tcp_emu() due to uninitialized stack variables
- BZ - 1728358 - Update qemu-kvm-rhev for RHEL 7.7 compatibility [OSP-14]
- BZ - 1728359 - Update qemu-kvm-rhev for RHEL 7.7 compatibility [OSP-13]
- BZ - 1728360 - Update qemu-kvm-rhev for RHEL 7.7 compatibility [OSP-10]

CVEs

- CVE-2018-15746
- CVE-2018-17958
- CVE-2018-17963
- CVE-2019-6501
- CVE-2019-6778
- CVE-2019-9824

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/.