[RHSA-2018:1113-01] Moderate: qemu-kvm-rhev security an...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=13977

Author
SecurityHome.eu

Published: 11 April 2018

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

==========
Red Hat Security Advisory

Synopsis: Moderate: qemu-kvm-rhev security and bug fix update
Advisory ID: RHSA-2018:1113-01
Product: Red Hat Enterprise Linux OpenStack Platform
Advisory URL: https://access.redhat.com/errata/RHSA-2018:1113
Issue date: 2018-04-11
CVE Names: CVE-2017-13672 CVE-2017-13673 CVE-2017-13711
CVE-2017-15119 CVE-2017-15124
==========

1. Summary:

An update for qemu-kvm-rhev is now available for Red Hat OpenStack Platform 10.0 (Newton), Red Hat OpenStack Platform 11.0 (Ocata), Red Hat OpenStack Platform 12.0 (Pike), Red Hat OpenStack Platform 8.0 (Liberty), and Red Hat OpenStack Platform 9.0 (Mitaka).

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.

2. Relevant releases/architectures:

Red Hat OpenStack Platform 10.0 - x86_64
Red Hat OpenStack Platform 11.0 - x86_64
Red Hat OpenStack Platform 12.0 - ppc64le, x86_64
Red Hat OpenStack Platform 8.0 (Liberty) - x86_64

Red Hat OpenStack Platform 9.0 - x86_64

3. 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):

* The Network Block Device (NBD) server in Quick Emulator (QEMU), is vulnerable to a denial of service issue. It could occur if a client sent large option requests, making the server waste CPU time on reading up to 4GB per request. A client could use this flaw to keep the NBD server from serving other requests, resulting in DoS. (CVE-2017-15119)

* Qemu: vga: OOB read access during display update (CVE-2017-13672)

* Qemu: vga: reachable assert failure during display update (CVE-2017-13673)

* Qemu: Slirp: use-after-free when sending response (CVE-2017-13711)

* VNC server implementation in Quick Emulator (QEMU) was found to be vulnerable to an unbounded memory allocation issue, as it did not throttle the framebuffer updates sent to its client. If the client did not consume these updates, VNC server allocates growing memory to hold onto this data. A malicious remote VNC client could use this flaw to cause DoS to the server host. (CVE-2017-15124)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

Red Hat would like to thank David Buchanan for reporting CVE-2017-13672 and CVE-2017-13673 and Wjjzhang (Tencent.com) for reporting CVE-2017-13711. The CVE-2017-15119 issue was discovered by Eric Blake (Red Hat) and the CVE-2017-15124 issue was discovered by Daniel Berrange (Red Hat).

4. 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.

5. Bugs fixed (https://bugzilla.redhat.com/):

1486400 - CVE-2017-13711 Qemu: Slirp: use-after-free when sending response
1486560 - CVE-2017-13672 Qemu: vga: OOB read access during display update
1486588 - CVE-2017-13673 Qemu: vga: reachable assert failure during display update
1516925 - CVE-2017-15119 qemu: DoS via large option request
1525195 - CVE-2017-15124 Qemu: memory exhaustion through framebuffer update request message in VNC server
1549860 - Update qemu-kvm-rhev for RHEL 7.5 compatibility [osp-11]
1553107 - Update qemu-kvm-rhev for RHEL 7.5 compatibility [osp-10]
1557010 - Update qemu-kvm-rhev for RHEL 7.5 compatibility [osp-9]
1557011 - Update qemu-kvm-rhev for RHEL 7.5 compatibility [osp-8]
1562826 - Update qemu-kvm-rhev for RHEL 7.5 compatibility [osp-12]

6. Package List:

Red Hat OpenStack Platform 10.0:

Source:
qemu-kvm-rhev-2.10.0-21.el7.src.rpm

x86_64:
qemu-img-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-common-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-debuginfo-2.10.0-21.el7.x86_64.rpm
qemu-kvm-tools-rhev-2.10.0-21.el7.x86_64.rpm

Red Hat OpenStack Platform 11.0:

Source:
qemu-kvm-rhev-2.10.0-21.el7.src.rpm

x86_64:
qemu-img-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-common-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-debuginfo-2.10.0-21.el7.x86_64.rpm
qemu-kvm-tools-rhev-2.10.0-21.el7.x86_64.rpm

Red Hat OpenStack Platform 12.0:

Source:
qemu-kvm-rhev-2.10.0-21.el7.src.rpm

ppc64le:
qemu-img-rhev-2.10.0-21.el7.ppc64le.rpm
qemu-kvm-common-rhev-2.10.0-21.el7.ppc64le.rpm
qemu-kvm-rhev-2.10.0-21.el7.ppc64le.rpm
qemu-kvm-rhev-debuginfo-2.10.0-21.el7.ppc64le.rpm
qemu-kvm-tools-rhev-2.10.0-21.el7.ppc64le.rpm

x86_64:
qemu-img-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-common-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-debuginfo-2.10.0-21.el7.x86_64.rpm
qemu-kvm-tools-rhev-2.10.0-21.el7.x86_64.rpm

Red Hat OpenStack Platform 8.0 (Liberty):

Source:
qemu-kvm-rhev-2.10.0-21.el7.src.rpm

x86_64:
qemu-img-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-common-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-debuginfo-2.10.0-21.el7.x86_64.rpm
qemu-kvm-tools-rhev-2.10.0-21.el7.x86_64.rpm

Red Hat OpenStack Platform 9.0:

Source:
qemu-kvm-rhev-2.10.0-21.el7.src.rpm

x86_64:
qemu-img-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-common-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-2.10.0-21.el7.x86_64.rpm
qemu-kvm-rhev-debuginfo-2.10.0-21.el7.x86_64.rpm
qemu-kvm-tools-rhev-2.10.0-21.el7.x86_64.rpm

These packages are GPG signed by Red Hat for security. Our key and
details on how to verify the signature are available from
https://access.redhat.com/security/team/key/

7. References:

https://access.redhat.com/security/cve/CVE-2017-13672
https://access.redhat.com/security/cve/CVE-2017-13673
https://access.redhat.com/security/cve/CVE-2017-13711
https://access.redhat.com/security/cve/CVE-2017-15119

https://access.redhat.com/security/cve/CVE-2017-15124
https://access.redhat.com/security/updates/classification/#moderate

8. Contact:

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