[RHSA-2022:5939-01] Moderate: kernel-rt security and bu...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=21204

Author
SecurityHome.eu

Published: 09 August 2022

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

Synopsis: Moderate: kernel-rt security and bug fix update
Advisory ID: RHSA-2022:5939-01
Product: Red Hat Enterprise Linux
Advisory URL: https://access.redhat.com/errata/RHSA-2022:5939
Issue date: 2022-08-09
CVE Names: CVE-2022-21123 CVE-2022-21125 CVE-2022-21166
==========
1. Summary:

An update for kernel-rt is now available for Red Hat Enterprise Linux 7.

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 Enterprise Linux for Real Time (v. 7) - noarch, x86_64
Red Hat Enterprise Linux for Real Time for NFV (v. 7) - noarch, x86_64

3. Description:

The kernel-rt packages provide the Real Time Linux Kernel, which enables
fine-tuning for systems with extremely high determinism requirements.

Security Fix(es):

* Incomplete cleanup of multi-core shared buffers (aka SBDR)
(CVE-2022-21123)

* Incomplete cleanup of microarchitectural fill buffers (aka SBDS) (CVE-2022-21125)

* Incomplete cleanup in specific special register write operations (aka DRPW) (CVE-2022-21166)

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):

* The kernel-rt crashes where one task is indefinitely looping in __start_cfs_bandwidth() with the cfs_b->lock spinlock being held (BZ#2079976)

* update to the latest RHEL7.9.z16 source tree (BZ#2100182)

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

The system must be rebooted for this update to take effect.

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

2090237 - CVE-2022-21123 hw: cpu: Incomplete cleanup of multi-core shared buffers (aka SBDR)
2090240 - CVE-2022-21125 hw: cpu: Incomplete cleanup of microarchitectural fill buffers (aka SBDS)
2090241 - CVE-2022-21166 hw: cpu: Incomplete cleanup in specific special register write operations (aka DRPW)

6. Package List:

Red Hat Enterprise Linux for Real Time for NFV (v. 7):

Source:
kernel-rt-3.10.0-1160.76.1.rt56.1220.el7.src.rpm

noarch:
kernel-rt-doc-3.10.0-1160.76.1.rt56.1220.el7.noarch.rpm

x86_64:
kernel-rt-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm

kernel-rt-debug-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-devel-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-kvm-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-kvm-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debuginfo-common-x86_64-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-devel-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-kvm-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-kvm-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-devel-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-kvm-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-kvm-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm

Red Hat Enterprise Linux for Real Time (v. 7):

Source:
kernel-rt-3.10.0-1160.76.1.rt56.1220.el7.src.rpm

noarch:
kernel-rt-doc-3.10.0-1160.76.1.rt56.1220.el7.noarch.rpm

x86_64:
kernel-rt-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debug-devel-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-debuginfo-common-x86_64-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-devel-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-debuginfo-3.10.0-1160.76.1.rt56.1220.el7.x86_64.rpm
kernel-rt-trace-devel-3.10.0-1160.76.1.rt56.1220.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-2022-21123
https://access.redhat.com/security/cve/CVE-2022-21125
https://access.redhat.com/security/cve/CVE-2022-21166
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/