[RHSA-2022:5232-01] Important: kernel security and bug ...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=20961

Author
SecurityHome.eu

Published: 28 June 2022

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

Synopsis: Important: kernel security and bug fix update
Advisory ID: RHSA-2022:5232-01
Product: Red Hat Enterprise Linux
Advisory URL: https://access.redhat.com/errata/RHSA-2022:5232
Issue date: 2022-06-28
CVE Names: CVE-2022-1729 CVE-2022-1966
==========
1. Summary:

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

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.

2. Relevant releases/architectures:

Red Hat Enterprise Linux Client (v. 7) - noarch, x86_64
Red Hat Enterprise Linux Client Optional (v. 7) - x86_64
Red Hat Enterprise Linux ComputeNode (v. 7) - noarch, x86_64
Red Hat Enterprise Linux ComputeNode Optional (v. 7) - x86_64
Red Hat Enterprise Linux Server (v. 7) - noarch, ppc64, ppc64le, s390x, x86_64
Red Hat Enterprise Linux Server Optional (v. 7) - ppc64, ppc64le, x86_64
Red Hat Enterprise Linux Workstation (v. 7) - noarch, x86_64
Red Hat Enterprise Linux Workstation Optional (v. 7) - x86_64

3. Description:

The kernel packages contain the Linux kernel, the core of any Linux

operating system.

Security Fix(es):

* kernel: race condition in perf_event_open leads to privilege escalation (CVE-2022-1729)

* kernel: a use-after-free write in the netfilter subsystem can lead to privilege escalation to root (CVE-2022-1966)

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):

* XFS inode cluster corruption (BZ#2050464)

* sock: sock_dequeue_err_skb() needs hard irq safety (BZ#2070408)

* libceph: fix potential use-after-free on linger ping and resends (BZ#2088025)

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/):

2086753 - CVE-2022-1729 kernel: race condition in perf_event_open leads to privilege escalation
2092427 - CVE-2022-1966 kernel: a use-after-free write in the netfilter subsystem can lead to privilege escalation to root

6. Package List:

Red Hat Enterprise Linux Client (v. 7):

Source:
kernel-3.10.0-1160.71.1.el7.src.rpm

noarch:
kernel-abi-whitelists-3.10.0-1160.71.1.el7.noarch.rpm
kernel-doc-3.10.0-1160.71.1.el7.noarch.rpm

x86_64:
bpftool-3.10.0-1160.71.1.el7.x86_64.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64.rpm
perf-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux Client Optional (v. 7):

x86_64:
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-devel-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux ComputeNode (v. 7):

Source:
kernel-3.10.0-1160.71.1.el7.src.rpm

noarch:
kernel-abi-whitelists-3.10.0-1160.71.1.el7.noarch.rpm
kernel-doc-3.10.0-1160.71.1.el7.noarch.rpm

x86_64:
bpftool-3.10.0-1160.71.1.el7.x86_64.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.x86_64.rpm

kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64.rpm
perf-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux ComputeNode Optional (v. 7):

x86_64:
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-devel-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux Server (v. 7):

Source:
kernel-3.10.0-1160.71.1.el7.src.rpm

noarch:
kernel-abi-whitelists-3.10.0-1160.71.1.el7.noarch.rpm
kernel-doc-3.10.0-1160.71.1.el7.noarch.rpm

ppc64:
bpftool-3.10.0-1160.71.1.el7.ppc64.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-bootwrapper-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debug-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debuginfo-common-ppc64-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-devel-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-headers-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-tools-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.ppc64.rpm

perf-3.10.0-1160.71.1.el7.ppc64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
python-perf-3.10.0-1160.71.1.el7.ppc64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm

ppc64le:
bpftool-3.10.0-1160.71.1.el7.ppc64le.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-bootwrapper-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debug-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debuginfo-common-ppc64le-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-devel-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-headers-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-tools-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.ppc64le.rpm
perf-3.10.0-1160.71.1.el7.ppc64le.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
python-perf-3.10.0-1160.71.1.el7.ppc64le.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm

s390x:
bpftool-3.10.0-1160.71.1.el7.s390x.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.s390x.rpm
kernel-3.10.0-1160.71.1.el7.s390x.rpm
kernel-debug-3.10.0-1160.71.1.el7.s390x.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.s390x.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.s390x.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.s390x.rpm
kernel-debuginfo-common-s390x-3.10.0-1160.71.1.el7.s390x.rpm
kernel-devel-3.10.0-1160.71.1.el7.s390x.rpm
kernel-headers-3.10.0-1160.71.1.el7.s390x.rpm
kernel-kdump-3.10.0-1160.71.1.el7.s390x.rpm
kernel-kdump-debuginfo-3.10.0-1160.71.1.el7.s390x.rpm
kernel-kdump-devel-3.10.0-1160.71.1.el7.s390x.rpm
perf-3.10.0-1160.71.1.el7.s390x.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.s390x.rpm
python-perf-3.10.0-1160.71.1.el7.s390x.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.s390x.rpm

x86_64:
bpftool-3.10.0-1160.71.1.el7.x86_64.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-3.10.0-1160.71.1.el7.x86_64.rpm

kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64.rpm
perf-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux Server Optional (v. 7):

ppc64:
bpftool-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-debuginfo-common-ppc64-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
kernel-tools-libs-devel-3.10.0-1160.71.1.el7.ppc64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.ppc64.rpm

ppc64le:
bpftool-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-debuginfo-common-ppc64le-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
kernel-tools-libs-devel-3.10.0-1160.71.1.el7.ppc64le.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.ppc64le.rpm

x86_64:
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-devel-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux Workstation (v. 7):

Source:
kernel-3.10.0-1160.71.1.el7.src.rpm

noarch:
kernel-abi-whitelists-3.10.0-1160.71.1.el7.noarch.rpm
kernel-doc-3.10.0-1160.71.1.el7.noarch.rpm

x86_64:
bpftool-3.10.0-1160.71.1.el7.x86_64.rpm
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64.rpm
perf-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm

Red Hat Enterprise Linux Workstation Optional (v. 7):

x86_64:
bpftool-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debug-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
kernel-tools-libs-devel-3.10.0-1160.71.1.el7.x86_64.rpm
perf-debuginfo-3.10.0-1160.71.1.el7.x86_64.rpm
python-perf-debuginfo-3.10.0-1160.71.1.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-2022-1729
https://access.redhat.com/security/cve/CVE-2022-1966
https://access.redhat.com/security/updates/classification/#important

8. Contact:

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