

## [RHSA-2022:4745-01] Important: rh-varnish6-varnish secu...

Article URL

[www.securityhome.eu/mailings/mailling.php?mid=20757](http://www.securityhome.eu/mailings/mailling.php?mid=20757)

Author

SecurityHome.eu

Published: 26 May 2022

---

=====  
Red Hat Security Advisory

Synopsis: Important: rh-varnish6-varnish security update  
Advisory ID: RHSA-2022:4745-01  
Product: Red Hat Software Collections  
Advisory URL: <https://access.redhat.com/errata/RHSA-2022:4745>  
Issue date: 2022-05-25  
CVE Names: CVE-2022-23959

=====

### 1. Summary:

An update for rh-varnish6-varnish is now available for Red Hat Software Collections.

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 Software Collections for Red Hat Enterprise Linux Server (v. 7) - ppc64le, s390x, x86\_64  
Red Hat Software Collections for Red Hat Enterprise Linux Workstation (v. 7) - x86\_64

### 3. Description:

Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

### Security Fix(es):

\* varnish: HTTP/1 request smuggling vulnerability (CVE-2022-23959)

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.

#### 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>

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

2045031 - CVE-2022-23959 varnish: HTTP/1 request smuggling vulnerability

#### 6. Package List:

Red Hat Software Collections for Red Hat Enterprise Linux Server (v. 7):

Source:

rh-varnish6-varnish-6.0.8-2.el7.1.src.rpm

ppc64le:

rh-varnish6-varnish-6.0.8-2.el7.1.ppc64le.rpm

rh-varnish6-varnish-devel-6.0.8-2.el7.1.ppc64le.rpm

rh-varnish6-varnish-docs-6.0.8-2.el7.1.ppc64le.rpm

rh-varnish6-varnish-libs-6.0.8-2.el7.1.ppc64le.rpm

s390x:

rh-varnish6-varnish-6.0.8-2.el7.1.s390x.rpm

rh-varnish6-varnish-devel-6.0.8-2.el7.1.s390x.rpm

rh-varnish6-varnish-docs-6.0.8-2.el7.1.s390x.rpm

rh-varnish6-varnish-libs-6.0.8-2.el7.1.s390x.rpm

x86\_64:

rh-varnish6-varnish-6.0.8-2.el7.1.x86\_64.rpm

rh-varnish6-varnish-devel-6.0.8-2.el7.1.x86\_64.rpm

rh-varnish6-varnish-docs-6.0.8-2.el7.1.x86\_64.rpm

rh-varnish6-varnish-libs-6.0.8-2.el7.1.x86\_64.rpm

Red Hat Software Collections for Red Hat Enterprise Linux Workstation (v. 7):

Source:

rh-varnish6-varnish-6.0.8-2.el7.1.src.rpm

x86\_64:

rh-varnish6-varnish-6.0.8-2.el7.1.x86\_64.rpm  
rh-varnish6-varnish-devel-6.0.8-2.el7.1.x86\_64.rpm  
rh-varnish6-varnish-docs-6.0.8-2.el7.1.x86\_64.rpm  
rh-varnish6-varnish-libs-6.0.8-2.el7.1.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-2022-23959>  
<https://access.redhat.com/security/updates/classification/#important>

#### 8. Contact:

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

Copyright 2022 Red Hat, Inc.