

## [RHSA-2020:3475-01] Important: bind security update

Article URL

[www.securityhome.eu/mailings/mailling.php?mid=17503](http://www.securityhome.eu/mailings/mailling.php?mid=17503)

Author

SecurityHome.eu

Published: 18 August 2020

---

=====  
Red Hat Security Advisory

Synopsis: Important: bind security update  
Advisory ID: RHSA-2020:3475-01  
Product: Red Hat Enterprise Linux  
Advisory URL: <https://access.redhat.com/errata/RHSA-2020:3475>  
Issue date: 2020-08-18  
CVE Names: CVE-2020-8616 CVE-2020-8617

=====

### 1. Summary:

An update for bind is now available for Red Hat Enterprise Linux 7.6 Extended Update Support.

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 ComputeNode EUS (v. 7.6) - noarch, x86\_64  
Red Hat Enterprise Linux ComputeNode Optional EUS (v. 7.6) - x86\_64  
Red Hat Enterprise Linux Server EUS (v. 7.6) - noarch, ppc64, ppc64le, s390x, x86\_64  
Red Hat Enterprise Linux Server Optional EUS (v. 7.6) - ppc64, ppc64le, s390x, x86\_64  
Red Hat Enterprise Linux for ARM and IBM Power LE (POWER9) Server (v. 7) - aarch64, noarch, ppc64le, s390x  
Red Hat Enterprise Linux for ARM and IBM Power LE (POWER9) Server Optional (v. 7) - aarch64, ppc64le, s390x

### 3. Description:

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

#### Security Fix(es):

\* bind: BIND does not sufficiently limit the number of fetches performed when processing referrals (CVE-2020-8616)

\* bind: A logic error in code which checks TSIG validity can be used to trigger an assertion failure in tsig.c (CVE-2020-8617)

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>

After installing the update, the BIND daemon (named) will be restarted automatically.

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

1836118 - CVE-2020-8616 bind: BIND does not sufficiently limit the number of fetches performed when processing referrals

1836124 - CVE-2020-8617 bind: A logic error in code which checks TSIG validity can be used to trigger an assertion failure in tsig.c

#### 6. Package List:

Red Hat Enterprise Linux ComputeNode EUS (v. 7.6):

##### Source:

bind-9.9.4-74.el7\_6.4.src.rpm

##### noarch:

bind-license-9.9.4-74.el7\_6.4.noarch.rpm

##### x86\_64:

bind-debuginfo-9.9.4-74.el7\_6.4.i686.rpm

bind-debuginfo-9.9.4-74.el7\_6.4.x86\_64.rpm

bind-libs-9.9.4-74.el7\_6.4.i686.rpm

bind-libs-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.i686.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-utils-9.9.4-74.el7\_6.4.x86\_64.rpm

Red Hat Enterprise Linux ComputeNode Optional EUS (v. 7.6):

x86\_64:  
bind-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-chroot-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.i686.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-devel-9.9.4-74.el7\_6.4.i686.rpm  
bind-devel-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.i686.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.i686.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.i686.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-utils-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-sdb-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-sdb-chroot-9.9.4-74.el7\_6.4.x86\_64.rpm

Red Hat Enterprise Linux Server EUS (v. 7.6):

Source:  
bind-9.9.4-74.el7\_6.4.src.rpm

noarch:  
bind-license-9.9.4-74.el7\_6.4.noarch.rpm

ppc64:  
bind-9.9.4-74.el7\_6.4.ppc64.rpm  
bind-chroot-9.9.4-74.el7\_6.4.ppc64.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.ppc.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.ppc64.rpm  
bind-libs-9.9.4-74.el7\_6.4.ppc.rpm  
bind-libs-9.9.4-74.el7\_6.4.ppc64.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.ppc.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.ppc64.rpm  
bind-utils-9.9.4-74.el7\_6.4.ppc64.rpm

ppc64le:  
bind-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-chroot-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-libs-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-pkcs11-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-pkcs11-utils-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-utils-9.9.4-74.el7\_6.4.ppc64le.rpm

s390x:

bind-9.9.4-74.el7\_6.4.s390x.rpm  
bind-chroot-9.9.4-74.el7\_6.4.s390x.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.s390.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.s390x.rpm  
bind-libs-9.9.4-74.el7\_6.4.s390.rpm  
bind-libs-9.9.4-74.el7\_6.4.s390x.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.s390.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.s390x.rpm  
bind-utils-9.9.4-74.el7\_6.4.s390x.rpm

x86\_64:

bind-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-chroot-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.i686.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-libs-9.9.4-74.el7\_6.4.i686.rpm  
bind-libs-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.i686.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.i686.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-utils-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-utils-9.9.4-74.el7\_6.4.x86\_64.rpm

Red Hat Enterprise Linux for ARM and IBM Power LE (POWER9) Server (v. 7):

Source:

bind-9.9.4-74.el7\_6.4.src.rpm

aarch64:

bind-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-chroot-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-libs-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-libs-lite-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-pkcs11-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-pkcs11-utils-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-utils-9.9.4-74.el7\_6.4.aarch64.rpm

noarch:

bind-license-9.9.4-74.el7\_6.4.noarch.rpm

ppc64le:

bind-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-chroot-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-debuginfo-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-libs-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-libs-lite-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-pkcs11-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-pkcs11-libs-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-pkcs11-utils-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-utils-9.9.4-74.el7\_6.4.ppc64le.rpm

s390x:

bind-9.9.4-74.el7\_6.4.s390x.rpm

bind-chroot-9.9.4-74.el7\_6.4.s390x.rpm

bind-debuginfo-9.9.4-74.el7\_6.4.s390.rpm

bind-debuginfo-9.9.4-74.el7\_6.4.s390x.rpm

bind-libs-9.9.4-74.el7\_6.4.s390.rpm

bind-libs-9.9.4-74.el7\_6.4.s390x.rpm

bind-libs-lite-9.9.4-74.el7\_6.4.s390.rpm

bind-libs-lite-9.9.4-74.el7\_6.4.s390x.rpm

bind-utils-9.9.4-74.el7\_6.4.s390x.rpm

Red Hat Enterprise Linux Server Optional EUS (v. 7.6):

ppc64:

bind-debuginfo-9.9.4-74.el7\_6.4.ppc.rpm

bind-debuginfo-9.9.4-74.el7\_6.4.ppc64.rpm

bind-devel-9.9.4-74.el7\_6.4.ppc.rpm

bind-devel-9.9.4-74.el7\_6.4.ppc64.rpm

bind-lite-devel-9.9.4-74.el7\_6.4.ppc.rpm

bind-lite-devel-9.9.4-74.el7\_6.4.ppc64.rpm

bind-pkcs11-9.9.4-74.el7\_6.4.ppc64.rpm

bind-pkcs11-devel-9.9.4-74.el7\_6.4.ppc.rpm

bind-pkcs11-devel-9.9.4-74.el7\_6.4.ppc64.rpm

bind-pkcs11-libs-9.9.4-74.el7\_6.4.ppc.rpm

bind-pkcs11-libs-9.9.4-74.el7\_6.4.ppc64.rpm

bind-pkcs11-utils-9.9.4-74.el7\_6.4.ppc64.rpm

bind-sdb-9.9.4-74.el7\_6.4.ppc64.rpm

bind-sdb-chroot-9.9.4-74.el7\_6.4.ppc64.rpm

ppc64le:

bind-debuginfo-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-devel-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-lite-devel-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-pkcs11-devel-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-sdb-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-sdb-chroot-9.9.4-74.el7\_6.4.ppc64le.rpm

s390x:

bind-debuginfo-9.9.4-74.el7\_6.4.s390.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.s390x.rpm  
bind-devel-9.9.4-74.el7\_6.4.s390.rpm  
bind-devel-9.9.4-74.el7\_6.4.s390x.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.s390.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.s390.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.s390.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-utils-9.9.4-74.el7\_6.4.s390x.rpm  
bind-sdb-9.9.4-74.el7\_6.4.s390x.rpm  
bind-sdb-chroot-9.9.4-74.el7\_6.4.s390x.rpm

x86\_64:

bind-debuginfo-9.9.4-74.el7\_6.4.i686.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-devel-9.9.4-74.el7\_6.4.i686.rpm  
bind-devel-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.i686.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.i686.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-sdb-9.9.4-74.el7\_6.4.x86\_64.rpm  
bind-sdb-chroot-9.9.4-74.el7\_6.4.x86\_64.rpm

Red Hat Enterprise Linux for ARM and IBM Power LE (POWER9) Server Optional (v. 7):

aarch64:

bind-debuginfo-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-devel-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-sdb-9.9.4-74.el7\_6.4.aarch64.rpm  
bind-sdb-chroot-9.9.4-74.el7\_6.4.aarch64.rpm

ppc64le:

bind-debuginfo-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-devel-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.ppc64le.rpm  
bind-sdb-9.9.4-74.el7\_6.4.ppc64le.rpm

bind-sdb-chroot-9.9.4-74.el7\_6.4.ppc64le.rpm

s390x:

bind-debuginfo-9.9.4-74.el7\_6.4.s390.rpm  
bind-debuginfo-9.9.4-74.el7\_6.4.s390x.rpm  
bind-devel-9.9.4-74.el7\_6.4.s390.rpm  
bind-devel-9.9.4-74.el7\_6.4.s390x.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.s390.rpm  
bind-lite-devel-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.s390.rpm  
bind-pkcs11-devel-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.s390.rpm  
bind-pkcs11-libs-9.9.4-74.el7\_6.4.s390x.rpm  
bind-pkcs11-utils-9.9.4-74.el7\_6.4.s390x.rpm  
bind-sdb-9.9.4-74.el7\_6.4.s390x.rpm  
bind-sdb-chroot-9.9.4-74.el7\_6.4.s390x.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-2020-8616>  
<https://access.redhat.com/security/cve/CVE-2020-8617>  
<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 2020 Red Hat, Inc.