

## [RHSA-2021:0922-01] Important: bind security update

Article URL

[www.securityhome.eu/mailings/mailling.php?mid=18594](http://www.securityhome.eu/mailings/mailling.php?mid=18594)

Author

SecurityHome.eu

Published: 17 March 2021

---

=====  
Red Hat Security Advisory

Synopsis: Important: bind security update  
Advisory ID: RHSA-2021:0922-01  
Product: Red Hat Enterprise Linux  
Advisory URL: <https://access.redhat.com/errata/RHSA-2021:0922>  
Issue date: 2021-03-17  
CVE Names: CVE-2020-8625

=====

### 1. Summary:

An update for bind is now available for Red Hat Enterprise Linux 8.2 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 AppStream EUS (v. 8.2) - aarch64, noarch, ppc64le, s390x, x86\_64  
Red Hat Enterprise Linux BaseOS EUS (v. 8.2) - aarch64, ppc64le, s390x, x86\_64

### 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: Buffer overflow in the SPNEGO implementation affecting GSSAPI security policy negotiation (CVE-2020-8625)

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/>):

1928486 - CVE-2020-8625 bind: Buffer overflow in the SPNEGO implementation affecting GSSAPI security policy negotiation

#### 6. Package List:

Red Hat Enterprise Linux AppStream EUS (v. 8.2):

aarch64:

bind-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-chroot-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-devel-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-libs-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-libs-lite-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-lite-devel-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-devel-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-libs-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-utils-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-sdb-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-sdb-chroot-9.11.13-6.el8\_2.2.aarch64.rpm

bind-sdb-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-utils-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm

noarch:

bind-license-9.11.13-6.el8\_2.2.noarch.rpm  
python3-bind-9.11.13-6.el8\_2.2.noarch.rpm

ppc64le:

bind-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-chroot-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-devel-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-libs-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-libs-lite-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-lite-devel-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-devel-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-libs-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-utils-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-sdb-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-sdb-chroot-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-utils-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm

s390x:

bind-9.11.13-6.el8\_2.2.s390x.rpm  
bind-chroot-9.11.13-6.el8\_2.2.s390x.rpm  
bind-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.s390x.rpm  
bind-devel-9.11.13-6.el8\_2.2.s390x.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-libs-9.11.13-6.el8\_2.2.s390x.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-libs-lite-9.11.13-6.el8\_2.2.s390x.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-lite-devel-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-devel-9.11.13-6.el8\_2.2.s390x.rpm

bind-pkcs11-libs-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-utils-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-sdb-9.11.13-6.el8\_2.2.s390x.rpm  
bind-sdb-chroot-9.11.13-6.el8\_2.2.s390x.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-utils-9.11.13-6.el8\_2.2.s390x.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm

x86\_64:

bind-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-chroot-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.i686.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-devel-9.11.13-6.el8\_2.2.i686.rpm  
bind-devel-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-libs-9.11.13-6.el8\_2.2.i686.rpm  
bind-libs-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-libs-lite-9.11.13-6.el8\_2.2.i686.rpm  
bind-libs-lite-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-lite-devel-9.11.13-6.el8\_2.2.i686.rpm  
bind-lite-devel-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-devel-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-devel-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-libs-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-libs-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-utils-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-sdb-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-sdb-chroot-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-utils-9.11.13-6.el8\_2.2.x86\_64.rpm

bind-utils-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm

Red Hat Enterprise Linux BaseOS EUS (v. 8.2):

Source:

bind-9.11.13-6.el8\_2.2.src.rpm

aarch64:

bind-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-export-devel-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-export-libs-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.aarch64.rpm

ppc64le:

bind-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-export-devel-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-export-libs-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.ppc64le.rpm

s390x:

bind-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.s390x.rpm  
bind-export-devel-9.11.13-6.el8\_2.2.s390x.rpm  
bind-export-libs-9.11.13-6.el8\_2.2.s390x.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm

bind-utils-debuginfo-9.11.13-6.el8\_2.2.s390x.rpm

x86\_64:

bind-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.i686.rpm  
bind-debugsource-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-export-devel-9.11.13-6.el8\_2.2.i686.rpm  
bind-export-devel-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-export-libs-9.11.13-6.el8\_2.2.i686.rpm  
bind-export-libs-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-export-libs-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-libs-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-libs-lite-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-libs-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-pkcs11-utils-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-sdb-debuginfo-9.11.13-6.el8\_2.2.x86\_64.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.i686.rpm  
bind-utils-debuginfo-9.11.13-6.el8\_2.2.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-2020-8625>  
<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 2021 Red Hat, Inc.