

[RHSA-2021:1475-01] Important: bind security update

Article URL

www.securityhome.eu/mailings/mailling.php?mid=18796

Author

SecurityHome.eu

Published: 03 May 2021

=====
Red Hat Security Advisory

Synopsis: Important: bind security update
Advisory ID: RHSA-2021:1475-01
Product: Red Hat Enterprise Linux
Advisory URL: <https://access.redhat.com/errata/RHSA-2021:1475>
Issue date: 2021-05-03
CVE Names: CVE-2021-25215

=====

1. Summary:

An update for bind is now available for Red Hat Enterprise Linux 7.3 Advanced 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 Server AUS (v. 7.3) - noarch, x86_64
Red Hat Enterprise Linux Server Optional AUS (v. 7.3) - 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: An assertion check can fail while answering queries for DNAME records that require the DNAME to be processed to resolve itself (CVE-2021-25215)

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/>):

1953857 - CVE-2021-25215 bind: An assertion check can fail while answering queries for DNAME records that require the DNAME to be processed to resolve itself

6. Package List:

Red Hat Enterprise Linux Server AUS (v. 7.3):

Source:

bind-9.9.4-50.el7_3.6.src.rpm

noarch:

bind-license-9.9.4-50.el7_3.6.noarch.rpm

x86_64:

bind-9.9.4-50.el7_3.6.x86_64.rpm

bind-chroot-9.9.4-50.el7_3.6.x86_64.rpm

bind-debuginfo-9.9.4-50.el7_3.6.i686.rpm

bind-debuginfo-9.9.4-50.el7_3.6.x86_64.rpm

bind-libs-9.9.4-50.el7_3.6.i686.rpm

bind-libs-9.9.4-50.el7_3.6.x86_64.rpm

bind-libs-lite-9.9.4-50.el7_3.6.i686.rpm

bind-libs-lite-9.9.4-50.el7_3.6.x86_64.rpm

bind-pkcs11-9.9.4-50.el7_3.6.x86_64.rpm

bind-pkcs11-libs-9.9.4-50.el7_3.6.i686.rpm

bind-pkcs11-libs-9.9.4-50.el7_3.6.x86_64.rpm

bind-pkcs11-utils-9.9.4-50.el7_3.6.x86_64.rpm

bind-utils-9.9.4-50.el7_3.6.x86_64.rpm

Red Hat Enterprise Linux Server Optional AUS (v. 7.3):

x86_64:

bind-debuginfo-9.9.4-50.el7_3.6.i686.rpm
bind-debuginfo-9.9.4-50.el7_3.6.x86_64.rpm
bind-devel-9.9.4-50.el7_3.6.i686.rpm
bind-devel-9.9.4-50.el7_3.6.x86_64.rpm
bind-lite-devel-9.9.4-50.el7_3.6.i686.rpm
bind-lite-devel-9.9.4-50.el7_3.6.x86_64.rpm
bind-pkcs11-devel-9.9.4-50.el7_3.6.i686.rpm
bind-pkcs11-devel-9.9.4-50.el7_3.6.x86_64.rpm
bind-sdb-9.9.4-50.el7_3.6.x86_64.rpm
bind-sdb-chroot-9.9.4-50.el7_3.6.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-2021-25215>
<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/>

Copyright 2021 Red Hat, Inc.