November 23, 2010

Contents

1 Introduction

BIND 9.6-ESV-R3 is a maintenance release for BIND 9.6-ESV.

This document summarizes changes from BIND 9.6-ESV-R1 to BIND 9.6-ESV-R3. Please see the CHANGES file in the source code release for a complete list of all changes.

2 Download

The latest release of BIND 9 software can always be found on our web site at http://www.isc.org/-software/bind. There you will find additional information about each release, source code, and some pre-compiled versions for certain operating systems.

3 Support

Product support information is available on http://www.isc.org/services/support for paid support options. Free support is provided by our user community via a mailing list. Information on all public email lists is available at https://lists.isc.org/mailman/listinfo.

4 New Features

4.1 9.6-ESV-R2

None.

4.2 9.6-ESV-R3

None.

5 Feature Changes

5.1 9.6-ESV-R2

None.

5.2 9.6-ESV-R3

None.

6 Security Fixes

6.1 9.6-ESV-R2

None.

6.2 9.6-ESV-R3

- Adding a NO DATA signed negative response to cache failed to clear any matching RRSIG records already in cache. A subsequent lookup of the cached NO DATA entry could crash named (INSIST) when the unexpected RRSIG was

also returned with the NO DATA cache entry. [RT #22288] [CVE-2010-3613] [VU#706148]

- BIND, acting as a DNSSEC validator, was determining if the NS RRset is insecure based on a value that could mean either that the RRset is actually insecure or that there wasn't a matching key for the RRSIG in the DNSKEY RRset when resuming from validating the DNSKEY RRset. This can happen when in the middle of a DNSKEY algorithm rollover, when two different algorithms were used to sign a zone but only the new set of keys are in the zone DNSKEY RRset. [RT #22309] [CVE-2010-3614] [VU#837744]

7 Bug Fixes

7.1 9.6-ESV-R2

- Check that named successfully skips NSEC3 records that fail to match the NSEC3PARAM record currently in use. [RT #21868]
- Worked around a race condition in the cache database memory handling. Without this fix a DNS cache DB or ADB could incorrectly stay in an over memory state, effectively refusing further caching, which subsequently made a BIND 9 caching server unworkable. [RT #21818]
- BIND did not properly handle non-cacheable negative responses from insecure zones. This caused several non-protocol-compliant zones to become unresolvable. BIND is now more accepting of responses it receives from less strict servers. [RT #21555]
- The resolver could attempt to destroy a fetch context too soon, resulting in a crash. [RT #19878]
- The placeholder negative caching element was not properly constructed triggering a crash (INSIST) in dns_ncache_towire(). [RT #21346]
- Handle the introduction of new trusted-keys and DS, DLV RRsets better. [RT #21097]
- Fix arguments to dns_keytable_findnextkeynode() call. [RT #20877]

7.2 9.6-ESV-R3

- Microsoft changed the behavior of sockets between NT/XP based stacks vs Vista/windows7 stacks. Server 2003/2008 have the older behavior, 2008r2 has the new behavior. With the change, different error results are possible, so ISC adapted BIND to handle the new error results. This resolves an issue where sockets would shut down on Windows servers causing named to stop responding to queries. [RT #21906]

- Windows has non-POSIX compliant behavior in its rename() and unlink() calls. This caused journal compaction to fail on Windows BIND servers with the log error: "dns_journal_compact failed: failure". [RT #22434]
- 'host -D' now turns on debugging messages earlier. [RT #22361]
- isc_print_vsnprintf() failed to check if there was space available in the buffer when adding a left justified character with a non zero width, (e.g. "%-1c"). [RT #22270]
- view->queryacl was being overloaded. Seperate the usage into view->queryacl, view->cacheacl and view->queryonacl. [RT #22114]
- win32: add more dependencies to BINDBuild.dsw. [RT #22062]
- win32: named-checkzone and named-checkconf failed to initialise winsock. [RT #21932]
- named failed to generate a correct signed response in a optout, delegation only zone with no secure delegations. [RT #22007]

8 Known issues in this release

- "make test" will fail on OSX and possibly other operating systems. The failure occurs in a new test to check for allow-query ACLs. The failure is caused because the source address is not specified on the dig commands issued in the test.

  If running "make test" is part of your usual acceptance process, please edit the file `bin/tests/system/allow_query/test.sh` and add

  `-b 10.53.0.2` to the `DIGOPTS` line.

9 Thank You

Thank you to everyone who assisted us in making this release possible. If you would like to contribute to ISC to assist us in continuing to make quality open source software, please visit our donations page at http://www.isc.org/supportisc.