January 28, 2011

Contents

1 Introduction

BIND 9.6.3 is the current release of BIND 9.6.

This document summarizes changes from BIND 9.6.2-P2 to BIND 9.6.3. Please see the CHANGES file in the source code release for a complete list of all changes.

2 Download

The latest development version of BIND 9 software can always be found on our web site at http://www.isc.org/downloads/development. 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 9.6.3

None.

5 Feature Changes

5.1 9.6.3

None.

6 Security Fixes

6.1 9.6.2-P3

- 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 9.6.3

- BIND now builds with threads disabled in versions of NetBSD earlier than 5.0 and with pthreads enabled by default in NetBSD versions 5.0 and higher. Also removes support for unproven-pthreads, mit-pthreads and ptl2. [RT #19203]

- HPUX now correctly defaults to using /dev/poll, which should increase performance. [RT #21919]
- If named is running as a threaded application, after an "rndc stop" command has been issued, other inbound TCP requests can cause named to hang and never complete shutdown. [RT #22108]
- When performing a GSS-TSIG signed dynamic zone update, memory could be leaked. This causes an unclean shutdown and may affect long-running servers. [RT #22573]
- A bug in NetBSD and FreeBSD kernels with SO_ACCEPTFILTER enabled allows for a TCP DoS attack. Until there is a kernel fix, ISC is disabling SO_ACCEPTFILTER support in BIND. [RT #22589]
- Corrected a defect where a combination of dynamic updates and zone transfers incorrectly locked the in-memory zone database, causing named to freeze. [RT #22614]
- Don't run MX checks (check-mx) when the MX record points to ".". [RT #22645]
- DST key reference counts can now be incremented via dst_key_attach. [RT #22672]
- isc_mutex_init_errcheck() in phtreads/mutex.c failed to destroy attr. [RT #22766]
- The Kerberos realm was being truncated when being pulled from the the host prinicipal, make krb5-self updates fail. [RT #22770]
- named failed to preserve the case of domain names in RDATA which is not compressible when writing master files. [RT #22863]
- There was a bug in how the clients-per-query code worked with some query patterns. This could result, in rare circumstances, in having all the client query slots filled with queries for the same DNS label, essentially ignoring the max-clients-per-query setting. [RT #22972]

7.2 9.6.2-P3

- 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]
- 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]

8 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.