January 20, 2011

Contents

1 Introduction

BIND 9.7.3rc1 is the first release candidate of BIND 9.7.3.

This document summarizes changes from BIND 9.7.1 to BIND 9.7.3. 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 9.7.2

- Zones may be dynamically added and removed with the "rndc addzone" and "rndc delzone" commands. These dynamically added zones are written to a per-view configuration file. Do not rely on the configuration file name nor contents as this will change in a future release. This is an experimental feature at this time.
- Added new "filter-aaaa-on-v4" access control list to select which IPv4 clients have AAAA record filtering applied.
- A new command "rndc secroots" was added to dump a combined summary of the currently managed keys combined with statically configured trust anchors.
- Added support to load new keys into managed zones without signing immediately with "rndc loadkeys". Added support to link keys with "dnssec-keygen -S" and "dnssec-settime -S".

5 Feature Changes

5.1 9.7.2

- Documentation improvements
- ORCHID prefixes were removed from the automatic empty zone list.
- Improved handling of GSSAPI security contexts. Specifically, better memory management of cached contexts, limited lifetime of a context to 1 hour, and added a "realm" command to nsupdate to allow selection of a non-default realm name.
- The contributed tool "zkt" was updated to version 1.0.

6 Security Fixes

6.1 9.7.2-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]

- When BIND is running as an authoritative server for a zone and receives a query for that zone data, it first checks for allow-query acls in the zone statement, then in that view, then in global options. If none of these exist, it defaults to allowing any query (allow-query {"any"};).

  With this bug, if the allow-query is not set in the zone statement, it failed to check in view or global options and fell back to the default of allowing any query. This means that queries that the zone owner did not wish to allow were incorrectly allowed. [RT #22418] [CVE-2010-3615] [VU#510208]

6.2 9.7.2-P2

- A flaw where the wrong ACL was applied was fixed. This flaw allowed access to a cache via recursion even though the ACL disallowed it.

6.3 9.7.2-P1

- If BIND, acting as a DNSSEC validating server, has two or more trust anchors configured in named.conf for the same zone (such as example.com) and the response for a record in that zone from the authoritative server includes a bad signature, the validating server will crash while trying to validate that query.

7 Bug Fixes

7.1 9.7.3

- 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]

- Added a regression test for fix 2896/RT #21045 ("rndc sign" failed to properly update the zone when adding a DNSKEY for publication only). [RT #21324]
- "nsupdate -l" now gives error message if "session.key" file is not found. [RT #21670]
- 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]
- An NSEC3PARAM record placed inside a zone which is not properly signed with NSEC3 could cause named to crash, if changed via dynamic update. [RT #22363]
- "rndc -h" now includes "loadkeys" option. [RT #22493]
- 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]
- "dnssec-settime -S" no longer tests prepublication interval validity when the interval is set to 0. [RT #22761]
- 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]

7.2 9.7.2-P3

- 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]

7.3 9.7.2-P1

- A bug, introduced in BIND 9.7.2, caused named to fail to start if a master zone file was unreadable or missing. This has been corrected in 9.7.2-P1.

- BIND previously accepted answers from authoritative servers that did not provide a "proper" response, such as not setting AA bit. BIND was changed to be more strict in what it accepted but this caused operational issues. This new strictness has been backed out in 9.7.2-P1.

7.4 9.7.2

- Removed a warning message when running BIND 9 under Windows for when a TCP connection was aborted. This is a common occurrence and the warning was extraneous.

- 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.

- Partially disabled change 2864 because it would cause infinite attempts of RRSIG queries.

- 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.

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.