June 15, 2011

Contents

1 Introduction

BIND 9.6-ESV-R5rc1 is the first release candidate of BIND 9.6-ESV-R5.

This document summarizes changes from BIND 9.6-ESV-R4 to BIND 9.6-ESV-R5rc1. 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/-downloads/all. 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-R5rc1

- Added a tool able to generate malformed packets to allow testing of how named handles them. [RT #24096]

5 Security Fixes

5.1 9.6-ESV-R5rc1

- Change #2912 (see CHANGES) exposed a latent bug in the DNS message processing code that could allow certain UPDATE requests to crash named. [RT #24777] [CVE-2011-2464]

- named, set up to be a caching resolver, is vulnerable to a user querying a domain with very large resource record sets (RRSets) when trying to negatively cache the response. Due to an off-by-one error, caching the response could cause named to crash. [RT #24650] [CVE-2011-1910]

6 Feature Changes

6.1 9.6-ESV-R5rc1

- Merged in the NetBSD ATF test framework (currently version 0.12) for development of future unit tests. Use configure --with-atf to build ATF internally or configure --with-atf=prefix to use an external copy. [RT #23209]

- Added more verbose error reporting from DLZ LDAP. [RT #23402]

- Replaced compile time constant with STDTIME_ON_32BITS. [RT #23587]

7 Bug Fixes

7.1 9.6-ESV-R5rc1

- Improved the mechanism for flagging database entries as negative cache records; the former method, RR type 0, could be ambiguous. [RT #24777]

- During RFC5011 processing some journal write errors were not detected. This could lead to managed-keys changes being committed but not recorded in the journal files, causing potential inconsistencies during later processing. [RT #20256]
- A potential NULL pointer deference in the DNS64 code could cause named to terminate unexpectedly. [RT #20256]
- A state variable relating to DNSSEC could fail to be set during some infrequently-executed code paths, allowing it to be used whilst in an unitialized state during cache updates, with unpredictable results. [RT #20256]
- A potential NULL pointer deference in DNSSEC signing code could cause named to terminate unexpectedly [RT #20256]
- Several cosmetic code changes were made to silence warnings generated by a static code analysis tool. [RT #20256]
- Cause named to terminate at startup or rndc reconfig reload to fail, if a log file specified in the conf file isn't a plain file. (RT #22771]
- After an external code review, a code cleanup was done. [RT #22521]
- named now forces the ADB cache time for glue related data to zero instead of relying on TTL. This corrects problematic behavior in cases where a server was authoritative for the A record of a nameserver for a delegated zone and was queried to recursively resolve records within that zone. [RT #22842]
- Fix the zonechecks system test to fail on error (warning in 9.6, fatal in 9.7) to match behaviour for 9.4. [RT #22905]
- Fixed precedence order bug with NS and DNAME records if both are present. (Also fixed timing of autosign test in 9.7+) [RT #23035]
- The secure zone update feature in named is based on the zone being signed and configured for dynamic updates. A bug in the ACL processing for "allow-update { none; };" resulted in a zone that is supposed to be static being treated as a dynamic zone. Thus, named would try to sign/re-sign that zone erroneously. [RT #23120]
- If a slave initiates a TSIG signed AXFR from the master and the master fails to correctly TSIG sign the final message, the slave would be left with the zone in an unclean state. named detected this error too late and named would crash with an INSIST. The order dependancy has been fixed. [RT #23254]
- If the server has an IPv6 address but does not have IPv6 connectivity to the internet, dig +trace could fail attempting to use IPv6 addresses. [RT #23297]
- Changing TTL did not cause dnssec-signzone to generate new signatures. [RT #23330]

- Have the validating resolver use RRSIG original TTL to compute validated RRset and RRSIG TTL. [RT #23332]
- In "make test" bin/tests/resolver, hold the socket manager lock while freeing the socket. [RT #23333]
- If named encountered a CNAME instead of a DS record when walking the chain of trust down from the trust anchor, it incorrectly stopped validating. [RT #23338]
- RRSIG records could have time stamps too far in the future. [RT #23356]
- named stores cached data in an in-memory database and keeps track of how recently the data is used with a heap. The heap is stored within the cache's memory space. Under a sustained high query load and with a small cache size, this could lead to the heap exhausting the cache space. This would result in cache misses and SERVFAILs, with named never releasing the cache memory the heap used up and never recovering. This fix removes the heap into its own memory space, preventing the heap from exhausting the cache space and allowing named to recover gracefully when the high query load abates. [RT #23371]
- If running on a powerpc CPU and with atomic operations enabled, named could lock up. Added sync instructions to the end of atomic operations. [RT #23469]
- If OpenSSL was built without engine support, named would have compile errors and fail to build. [RT #23473]
- Handle isc_event_allocate failures in t_tasks test. [RT #23572]
- ixfr-from-differences {master|slave}; failed to select the master/slave zones, resulting in on diff/journal file being created. [RT #23580]
- If a DNAME substitution failed, named returned NOERROR. The correct response should be YXDOMAIN. [RT #23591]
- Remove bin/tests/system/logfileconfig/ns1/named.conf and add setup.sh in order to resolve changing named.conf issue. [RT #23687]
- NOTIFY messages were not being sent when generating a NSEC3 chain incrementally. [RT #23702]
- Signatures for records at the zone apex could go stale due to an incorrect timer setting. [RT #23769]
- The autosign tests attempted to open ports within reserved ranges. Test now avoids those ports. [RT #23957]
- Clean up some cross-compiling issues and added two undocumented configure options, --with-gost and --with-rlimtype, to allow over-riding default settings (gost=no and rlimtype="long int") when cross-compiling. [RT #24367]

- When trying sign with NSEC3, if dnssec-signzone couldn't find the KSK, it would give an incorrect error "NSEC3 iterations too big for weakest DNSKEY strength" rather than the correct "failed to find keys at the zone apex: not found" [RT #24369]
- nsupdate could dump core on shutdown when using SIG(0) keys. [RT #24604]
- Named could fail to validate zones list in a DLV that validated insecure without using DLV and had DS records in the parent zone. [RT #24631]

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.