July 23, 2011

Contents

1 Introduction

BIND 9.4-ESV-R5 is the current production release of BIND 9.4.

This document summarizes changes from BIND 9.4-ESV-R4 to BIND 9.4-ESV-R5. 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 9.4-ESV-R5

None.

5 Feature Changes

5.1 9.4-ESV-R5

None.

6 Security Fixes

6.1 9.4-ESV-R5

- 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]
- 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]
- Change #2912 (see CHANGES) exposed a latent bug in the DNS message processing code that could allow certain UPDATE requests to crash named. This was fixed by disambiguating internal database representation vs DNS wire format data. [RT #24777] [CVE-2011-2464]

7 Bug Fixes

7.1 9.4-ESV-R5

- 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]
- Prior to this fix, when named was was writing a zone to disk (as slave, when resigning, etc.), it might not correctly preserve the case of domain name labels within RDATA, if the RDATA was not compressible. The result is that when reloading the zone from disk would, named could serve data that did not match the RRSIG for that data, due to case mismatch. named now correctly preserves case. After upgrading to fixed code, the operator should either resign the data (on the master) or delete the disk file on the slave and reload the zone. [RT #22863]
- 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]
- 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]
- 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]
- Fixed precedence order bug with NS and DNAME records if both are present. (Also fixed timing of autosign test in 9.7+) [RT #23035]
- Changing TTL did not cause dnssec-signzone to generate new signatures. [RT #23330]
- 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]
- 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]
- ixfr-from-differences {master|slave}; failed to select the master/slave zones, resulting in on diff/journal file being created. [RT #23580]

- Remove bin/tests/system/logfileconfig/ns1/named.conf and add setup.sh in order to resolve changing named.conf issue. [RT #23687]
- The autosign tests attempted to open ports within reserved ranges. Test now avoids those ports. [RT #23957]
- 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]
- A bug in FreeBSD kernels causes IPv6 UDP responses greater than 1280 bytes to not fragment as they should. Until there is a kernel fix, named will work around this by setting IPV6_USE_MIN_MTU on a per packet basis. [RT #24950]

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.