1 Release Notes for BIND Version 9.9.8-S1

1.1 Introduction

This document summarizes changes since the last production release of BIND on the corresponding major release branch.

1.2 Download

The latest versions of BIND 9 software can always be found at http://www.isc.org/downloads/. There you will find additional information about each release, source code, and pre-compiled versions for Microsoft Windows operating systems.

1.3 Security Fixes

- An incorrect boundary check in the OPENPGPKEY rdatatype could trigger an assertion failure. This flaw is disclosed in CVE-2015-5986. [RT #40286]

- A buffer accounting error could trigger an assertion failure when parsing certain malformed DNSSEC keys.

  This flaw was discovered by Hanno Böck of the Fuzzing Project, and is disclosed in CVE-2015-5722. [RT #40212]

- A specially crafted query could trigger an assertion failure in message.c.

  This flaw was discovered by Jonathan Foote, and is disclosed in CVE-2015-5477. [RT #40046]

- On servers configured to perform DNSSEC validation, an assertion failure could be triggered on answers from a specially configured server.

  This flaw was discovered by Breno Silveira Soares, and is disclosed in CVE-2015-4620. [RT #39795]

1.4 New Features

- New quotas have been added to limit the queries that are sent by recursive resolvers to authoritative servers experiencing denial-of-service attacks. When configured, these options can both reduce the harm done to authoritative servers and also avoid the resource exhaustion that can be experienced by recursives when they are being used as a vehicle for such an attack.

  NOTE: These options are not available by default; use **configure --enable-fetchlimit** to include them in the build.

  - `fetches-per-server` limits the number of simultaneous queries that can be sent to any single authoritative server. The configured value is a starting point; it is automatically adjusted downward if the server is partially or completely non-responsive. The algorithm used to adjust the quota can be configured via the `fetch-quota-params` option.
  - `fetches-per-zone` limits the number of simultaneous queries that can be sent for names within a single domain. (Note: Unlike "fetches-per-server", this value is not self-tuning.)

  Statistics counters have also been added to track the number of queries affected by these quotas.

- An **--enable-querytrace** configure switch is now available to enable very verbose query tracelogging. This option can only be set at compile time. This option has a negative performance impact and should be used only for debugging. [RT #37520]

- The following types have been implemented: CSYNC, NINFO, RKEY, SINK, TA, TALINK.

- EDNS COOKIE options content is now displayed as "COOKIE: <hexvalue>".

1.5 Feature Changes

- Large inline-signing changes should be less disruptive. Signature generation is now incrementally; the number of signatures to be generated in each quantum is controlled by "sig-signing-signatures `number`;". [RT #37927]

- Retrieving the local port range from net.ipv4.ip_local_port_range on Linux is now supported.

- Active Directory names of the form gc._msdcs.<forest> are now accepted as valid hostnames when using the `check-names` option. <forest> is still restricted to letters, digits and hyphens.

- Names containing rich text are now accepted as valid hostnames in PTR records in DNS-SD reverse lookup zones, as specified in RFC 6763. [RT #37889]

- The default preferred glue is now the address type of the transport the query was received over.

- On machines with 2 or more processors (CPU), the default value for the number of UDP listeners has been changed to the number of detected processors minus one.

1.6 Porting Changes

- The Microsoft Windows install tool **BINDInstall.exe** which requires a non-free version of Visual Studio to be built, now uses two files (lists of flags and files) created by the Configure perl script with all the needed information which were previously compiled in the binary. Read `win32utils/build.txt` for more details. [RT #38915]

1.7 Bug Fixes

- Asynchronous zone loads were not handled correctly when the zone load was already in progress; this could trigger a crash in zt.c. [RT #37573]

- A race during shutdown or reconfiguration could cause an assertion failure in mem.c. [RT #38979]

- Some answer formatting options didn't work correctly with **dig +short**. [RT #39291]

- Malformed records of some types, including NSAP and UNSPEC, could trigger assertion failures when loading text zone files. [RT #40274] [RT #40285]

- Fixed a possible crash in ratelimiter.c caused by NOTIFY messages being removed from the wrong rate limiter queue. [RT #40350]

- The default `rrset-order` of `random` was inconsistently applied. [RT #40456]

- BADVERS responses from broken authoritative name servers were not handled correctly. [RT #40427]

1.8 End of Life

The BIND 9.9 (Extended Support Version) will be supported until June, 2017. https://www.isc.org/-downloads/software-support-policy/

1.9 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/donate/.