1 Release Notes for BIND Version 9.10.3

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.
- **dig +ednsflags** can now be used to set yet-to-be-defined EDNS flags in DNS requests.
- **dig +[no]ednsnegotiation** can now be used enable / disable EDNS version negotiation.

- 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.

1.5 Feature Changes

- Large inline-signing changes should be less disruptive. Signature generation is now done incrementally; the number of signatures to be generated in each quantum is controlled by "sig-signing-signatures `number`;". [RT #37927]
- The experimental SIT extension now uses the EDNS COOKIE option code point (10) and is displayed as "COOKIE: <value>". The existing named.conf directives; "request-sit", "sit-secret" and "nosit-udp-size", are still valid and will be replaced by "send-cookie", "cookie-secret" and "nocookie-udp-size" in BIND 9.11. The existing dig directive "+sit" is still valid and will be replaced with "+cookie" in BIND 9.11.
- When retrying a query via TCP due to the first answer being truncated, **dig** will now correctly send the COOKIE value returned by the server in the prior response. [RT #39047]
- 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]

1.6 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]
- Several bugs have been fixed in the RPZ implementation:
  - Policy zones that did not specifically require recursion could be treated as if they did; consequently, setting **qname-wait-recurse no;** was sometimes ineffective. This has been corrected. In most configurations, behavioral changes due to this fix will not be noticeable. [RT #39229]
  - The server could crash if policy zones were updated (e.g. via **rndc reload** or an incoming zone transfer) while RPZ processing was still ongoing for an active query. [RT #39415]
  - On servers with one or more policy zones configured as slaves, if a policy zone updated during regular operation (rather than at startup) using a full zone reload, such as via AXFR, a bug could allow the RPZ summary data to fall out of sync, potentially leading to an assertion failure in rpz.c when further incremental updates were made to the zone, such as via IXFR. [RT #39567]

- The server could match a shorter prefix than what was available in CLIENT-IP policy triggers, and so, an unexpected action could be taken. This has been corrected. [RT #39481]
- The server could crash if a reload of an RPZ zone was initiated while another reload of the same zone was already in progress. [RT #39649]
- Query names could match against the wrong policy zone if wildcard records were present. [RT #40357]

1.7 End of Life

The end of life for BIND 9.10 is yet to be determined but will not be before BIND 9.12.0 has been released for 6 months. <https://www.isc.org/downloads/software-support-policy/>

1.8 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/donate/>.