1 Release Notes for BIND Version 9.10.2-P4

1.1 Introduction

This document summarizes changes since BIND 9.10.2:

BIND 9.10.2-P4 addresses security issues described in CVE-2015-5722 and CVE-2015-5986.

BIND 9.10.2-P3 addresses a security issue described in CVE-2015-5477.

BIND 9.10.2-P2 addresses a security issue described in CVE-2015-4620.

BIND 9.10.2-P1 addressed several bugs that have been identified in the BIND 9.10 implementation of response-policy zones (RPZ). The bugs are in code which optimizes searching through multiple policy zones. In some cases, they can cause RPZ to behave inefficiently by searching for query matches in more policy zones than are strictly necessary, or to behave unpredictably by failing to search a policy zone that should have been searched. In the worst case, they can lead to assertion failures, terminating **named**.

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 Böeck 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 #39795]
- 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

- None

1.5 Feature Changes

- None

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]
- 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]

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/>.