1 Release Notes for BIND Version 9.9.7-P3

1.1 Introduction

This document summarizes changes since BIND 9.9.7.

BIND 9.9.7-P2 addresses security issues described in CVE-2015-5722 and CVE-2015-5986.

BIND 9.9.7-P2 addresses a security issue described in CVE-2015-5477.

BIND 9.9.7-P1 addresses a security issue described in CVE-2015-4620.

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

- None

1.7 End of Life

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

1.8 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/>.