

# 1 Release Notes for BIND Version 9.9.9-P5

## 1.1 Introduction

This document summarizes changes since BIND 9.9.9:

BIND 9.9.9-P5 addresses the security issues described in CVE-2016-9131, CVE-2016-9147, CVE-2016-9444 and CVE-2016-9778.

BIND 9.9.9-P4 addresses the security issue described in CVE-2016-8864.

BIND 9.9.9-P3 addresses the security issue described in CVE-2016-2776.

BIND 9.9.9-P2 addresses the security issue described in CVE-2016-2775.

BIND 9.9.9-P1 addresses Windows installation issues and a race condition in the rbt/rbtdb implementation resulting in named exiting due to assertion failures being detected.

## 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

- A coding error in the `nxdomain-redirect` feature could lead to an assertion failure if the redirection namespace was served from a local authoritative data source such as a local zone or a DLZ instead of via recursive lookup. This flaw is disclosed in CVE-2016-9778. [RT #43837]
- Named could mishandle authority sections that were missing RRSIGs triggering an assertion failure. This flaw is disclosed in CVE-2016-9444. [RT # 43632]
- Named mishandled some responses where covering RRSIG records are returned without the requested data resulting in a assertion failure. This flaw is disclosed in CVE-2016-9147. [RT #43548]
- Named incorrectly tried to cache TKEY records which could trigger a assertion failure when there was a class mismatch. This flaw is disclosed in CVE-2016-9131. [RT #43522]
- It was possible to trigger assertions when processing a response. This flaw is disclosed in CVE-2016-8864. [RT #43465]
- It was possible to trigger a assertion when rendering a message using a specially crafted request. This flaw is disclosed in CVE-2016-2776. [RT #43139]
- `getrrsetbyname` with a non absolute name could trigger an infinite recursion bug in `lwresd` and `named` with `lwres` configured if when combined with a search list entry the resulting name is too long. This flaw is disclosed in CVE-2016-2775. [RT #42694]

## 1.4 New Features

- None.

## 1.5 Feature Changes

- None.

## 1.6 Porting Changes

- None.

## 1.7 Bug Fixes

- Windows installs were failing due to triggering UAC without the installation binary being signed.
- A race condition in `rbt/rbtdb` was leading to INSISTs being triggered.

## **1.8 End of Life**

BIND 9.9 (Extended Support Version) will be supported until December, 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/>.