1 Release Notes for BIND Version 9.9.9-P8

1.1 Introduction

This document summarizes changes since BIND 9.9.9:

BIND 9.9.9-P7 addresses the security issue described in CVE-2017-3136, and updates the built in trusted keys for the root zone.

BIND 9.9.9-P6 addresses the security issue described in CVE-2017-3135, and fixes a regression introduced in a prior security release.

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 New DNSSEC Root Key

ICANN is in the process of introducing a new Key Signing Key (KSK) for the global root zone. BIND has multiple methods for managing DNSSEC trust anchors, with somewhat different behaviors. If the root key is configured using the **managed-keys** statement, or if the pre-configured root key is enabled by using **dnssec-validation auto**, then BIND can keep keys up to date automatically. Servers configured in this way will roll seamlessly to the new key when it is published in the root zone. However, keys configured using the **trusted-keys** statement are not automatically maintained. If your server is performing DNSSEC validation and is configured using **trusted-keys**, you are advised to change your configuration before the root zone begins signing with the new KSK. This is currently scheduled for October 11, 2017.

This release includes an updated version of the `bind.keys` file containing the new root key. This file can also be downloaded from https://www.isc.org/bind-keys .

1.4 Security Fixes

- 'rndc ""' could trigger a assertion failure in named. This flaw is disclosed in (CVE-2017-3138). [RT #44924]

- Some chaining (i.e., type CNAME or DNAME) responses to upstream queries could trigger assertion failures. This flaw is disclosed in CVE-2017-3137. [RT #44734]

- **dns64** with **break-dnssec yes;** can result in an assertion failure. This flaw is disclosed in CVE-2017-3136. [RT #44653]

- If a server is configured with a response policy zone (RPZ) that rewrites an answer with local data, and is also configured for DNS64 address mapping, a NULL pointer can be read triggering a server crash. This flaw is disclosed in CVE-2017-3135. [RT #44434]

- **named** could mishandle authority sections with missing RRSIGs, triggering an assertion failure. This flaw is disclosed in CVE-2016-9444. [RT #43632]

- **named** mishandled some responses where covering RRSIG records were returned without the requested data, resulting in an assertion failure. This flaw is disclosed in CVE-2016-9147. [RT #43548]

- **named** incorrectly tried to cache TKEY records which could trigger an 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 responses containing answers of type DNAME. This flaw is disclosed in CVE-2016-8864. [RT #43465]

- It was possible to trigger an assertion when rendering a message using a specially crafted request. This flaw is disclosed in CVE-2016-2776. [RT #43139]

- Calling **getrrsetbyname()** with a non- absolute name could trigger an infinite recursion bug in **lwresd** or **named** with **lwres** configured if, when combined with a search list entry from `resolv.conf`, the resulting name is too long. This flaw is disclosed in CVE-2016-2775. [RT #42694]

1.5   Feature Changes

- None.

1.6   Porting Changes

- None.

1.7   Bug Fixes

- A synthesized CNAME record appearing in a response before the associated DNAME could be cached, when it should not have been. This was a regression introduced while addressing CVE-2016-8864. [RT #44318]

- 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/.