1 Release Notes for BIND Version 9.10.5rc3

1.1 Introduction

This document summarizes changes since the last production release on the BIND 9.10 branch. Please see the `CHANGES` file for a further list of bug fixes and other changes.

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]
- Added the ability to specify the maximum number of records permitted in a zone (`max-records #;`). This provides a mechanism to block overly large zone transfers, which is a potential risk with slave zones from other parties, as described in CVE-2016-6170. [RT #42143]
- 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 New Features

- **named** now provides feedback to the owners of zones which have trust anchors configured (**trusted-keys**, **managed-keys**, **dnssec-validation auto;** and **dnssec-lookaside auto;**) by sending a daily query which encodes the keyids of the configured trust anchors for the zone. This is controlled by **trust-anchor-telemetry** and defaults to yes.
- A new **tcp-only** option has been added to **server** clauses, to indicate that UDP should not be used when sending queries to a specified IP address or prefix.

1.6 Feature Changes

- The ISC DNSSEC Lookaside Validation (DLV) service is scheduled to be disabled in 2017. A warning is now logged when **named** is configured to use this service, either explicitly or via `dnssec-lookaside auto;`. [RT #42207]
- If an ACL is specified with an address prefix in which the prefix length is longer than the address portion (for example, 192.0.2.1/8), **named** will now log a warning. In future releases this will be a fatal configuration error. [RT #43367]

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]
- **named** could deadlock if multiple changes to NSEC/NSEC3 parameters for the same zone were being processed at the same time. [RT #42770]
- **named** could trigger an assertion when sending NOTIFY messages. [RT #44019]
- Fixed a crash when calling **rndc stats** on some Windows builds: some Visual Studio compilers generate code that crashes when the "%z" printf() format specifier is used. [RT #42380]
- Windows installs were failing due to triggering UAC without the installation binary being signed.
- A change in the internal binary representation of the RBT database node structure enabled a race condition to occur (especially when BIND was built with certain compilers or optimizer settings), leading to inconsistent database state which caused random assertion failures. [RT #42380]
- Referencing a nonexistent zone in a **response-policy** statement could cause an assertion failure during configuration. [RT #43787]
- **rndc addzone** could cause a crash when attempting to add a zone with a type other than **master** or **slave**. Such zones are now rejected. [RT #43665]
- **named** could hang when encountering log file names with large apparent gaps in version number (for example, when files exist called "logfile.0", "logfile.1", and "logfile.1482954169"). This is now handled correctly. [RT #38688]
- If a zone was updated while **named** was processing a query for nonexistent data, it could return out-of-sync NSEC3 records causing potential DNSSEC validation failure. [RT #43247]
- **named** could crash when loading a zone which had RRISG records whose expiry fields were far enough apart to cause an integer overflow when comparing them. [RT #40571]
- The **arpaname** and **named-rrchecker** commands were not installed into the correct **prefix**`/bin` directory. [RT #42910]
- When receiving a response from an authoritative server with a TTL value of zero, **named>** will now only use that response once, to answer the currently active clients that were waiting for it. Previously, such response could be cached and reused for up to one second. [RT #42142]
- **named-checkconf** now checks the **rate-limit** clause for correctness. [RT #42970]
- Corrected a bug in the **rndc** control channel that could allow a read past the end of a buffer, crashing **named**. Thanks to Lian Yihan for reporting this error.

1.8 Maintenance

- The built-in root hints have been updated to include IPv6 addresses for B.ROOT-SERVERS.NET (2001:500:84::b), E.ROOT-SERVERS.NET (2001:500:a8::e) and G.ROOT-SERVERS.NET (2001:500:12::d0d).

1.9 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/

1.10 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/.