1 Release Notes for BIND Version 9.11.1rc3

1.1 Introduction

This document summarizes changes since the last production release on the BIND 9.11 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 License Change

With the release of BIND 9.11.0, ISC changed to the open source license for BIND from the ISC license to the Mozilla Public License (MPL 2.0).

The MPL-2.0 license requires that if you make changes to licensed software (e.g. BIND) and distribute them outside your organization, that you publish those changes under that same license. It does not require that you publish or disclose anything other than the changes you made to our software.

This new requirement will not affect anyone who is using BIND without redistributing it, nor anyone redistributing it without changes, therefore this change will be without consequence for most individuals and organizations who are using BIND.

Those unsure whether or not the license change affects their use of BIND, or who wish to discuss how to comply with the license may contact ISC at https://www.isc.org/mission/contact/.

1.5 Security Fixes

- **rndc ""** could trigger an 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]
- 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 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]

1.6 Feature Changes

- **dnstap** now stores both the local and remote addresses for all messages, instead of only the remote address. The default output format for **dnstap-read** has been updated to include these addresses, with the initiating address first and the responding address second, separated by "-%gt;" or "%lt;-" to indicate in which direction the message was sent. [RT #43595]
- Expanded and improved the YAML output from **dnstap-read -y**: it now includes packet size and a detailed breakdown of message contents. [RT #43622] [RT #43642]
- 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]
- 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]

1.8 Maintenance

- The built-in root hints have been updated to include an IPv6 address (2001:500:12::d0d) for G.ROOT-SERVERS.NET.

1.9 Miscellaneous Notes

- Authoritative server support for the EDNS Client Subnet option (ECS), introduced in BIND 9.11.0, was based on an early version of the specification, and is now known to have incompatibilities with other ECS implementations. It is also inefficient, requiring a separate view for each answer, and is unable to correct for overlapping subnets in the configuration. It is intended for testing purposes but is not recommended for for production use. This was not made sufficiently clear in the documentation at the time of release.

1.10 End of Life

The end of life for BIND 9.11 is yet to be determined but will not be before BIND 9.13.0 has been released for 6 months. https://www.isc.org/downloads/software-support-policy/

1.11 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/.