1 Release Notes for BIND Version 9.9.10b1

1.1 Introduction

This document summarizes significant changes since the last production release of BIND on the corresponding major release 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 Security Fixes

- **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]

1.4 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]

1.5 Bug Fixes

- 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** command was 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]
- 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.
- Reverted a change to the query logging format that was inadvertently backported from the 9.11 branch. [RT #43238]

1.6 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).

1.7 End of Life

BIND 9.9 (Extended Support Version) will be supported until December, 2017. https://www.isc.org/downloads/soft 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/.