1 Release Notes for BIND Version 9.10.4

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

- 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 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]

- Duplicate EDNS COOKIE options in a response could trigger an assertion failure. This flaw is disclosed in CVE-2016-2088. [RT #41809]

- The resolver could abort with an assertion failure due to improper DNAME handling when parsing fetch reply messages. This flaw is disclosed in CVE-2016-1286. [RT #41753]

- Malformed control messages can trigger assertions in named and rndc. This flaw is disclosed in CVE-2016-1285. [RT #41666]

- Certain errors that could be encountered when printing out or logging an OPT record containing a CLIENT-SUBNET option could be mishandled, resulting in an assertion failure. This flaw is disclosed in CVE-2015-8705. [RT #41397]

- Specific APL data could trigger an INSIST. This flaw is disclosed in CVE-2015-8704. [RT #41396]

- Incorrect reference counting could result in an INSIST failure if a socket error occurred while performing a lookup. This flaw is disclosed in CVE-2015-8461. [RT#40945]

- Insufficient testing when parsing a message allowed records with an incorrect class to be be accepted, triggering a REQUIRE failure when those records were subsequently cached. This flaw is disclosed in CVE-2015-8000. [RT #40987]

1.4 New Features

- The following resource record types have been implemented: AVC, CSYNC, NINFO, RKEY, SINK, SMIMEA, TA, TALINK.

- Added a warning for a common misconfiguration involving forwarded RFC 1918 and IPv6 ULA (Universal Local Address) zones.

- Contributed software from Nominum is included in the source at contrib/dnsperf-2.1.0.0-1/. It includes dnsperf for measuring the performance of authoritative DNS servers, resperf for testing the resolution performance of a caching DNS server, resperf-report for generating a resperf report in HTML with gnuplot graphs, and queryparse to extract DNS queries from pcap capture files. This software is not installed by default with BIND.

- When loading a signed zone, **named** will now check whether an RRSIG's inception time is in the future, and if so, it will regenerate the RRSIG immediately. This helps when a system's clock needs to be reset backwards.

- **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.

1.5 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]

- Updated the compiled-in addresses for H.ROOT-SERVERS.NET and L.ROOT-SERVERS.NET.

- The default preferred glue is now the address type of the transport the query was received over.

- On machines with 2 or more processors (CPU), the default value for the number of UDP listeners has been changed to the number of detected processors minus one.

- Zone transfers now use smaller message sizes to improve message compression. This results in reduced network usage.

- named -V output now also includes operating system details.

1.6 Porting Changes

- The Microsoft Windows install tool **BINDInstall.exe** which requires a non-free version of Visual Studio to be built, now uses two files (lists of flags and files) created by the Configure perl script with all the needed information which were previously compiled in the binary. Read `win32utils/build.txt` for more details. [RT #38915]

1.7 Bug Fixes

- 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]

- **rndc flushtree** now works even if there wasn't a cached node at the specified name. [RT #41846]

- Don't emit records with zero TTL unless the records were received with a zero TTL. After being returned to waiting clients, the answer will be discarded from the cache. [RT #41687]

- For Windows platforms, the SIT (Source Identity Token) support was restored. (It was mistakenly partially replaced in a previous beta with new 9.11 COOKIE support.) [RT #41905]

- When deleting records from a zone database, interior nodes could be left empty but not deleted, damaging search performance afterward. [RT #40997] [RT #41941]

- The server could crash due to a use-after-free if a zone transfer timed out. [RT #41297]

- Authoritative servers that were marked as bogus (e.g. blackholed in configuration or with invalid addresses) were being queried anyway. [RT #41321]

- Some of the options for GeoIP ACLs, including "areacode", "metrocode", and "timezone", were incorrectly documented as "area", "metro" and "tz". Both the long and abbreviated versions are now accepted.

- Zones configured to use **map** format master files can't be used as policy zones because RPZ summary data isn't compiled when such zones are mapped into memory. This limitation may be fixed in a future release, but in the meantime it has been documented, and attempting to use such zones in **response-policy** statements is now a configuration error. [RT #38321]

1.8 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/

1.9 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/.