1 Release Notes for BIND Version 9.14.7

1.1 Introduction

BIND 9.14 is a stable branch of BIND. This document summarizes significant changes since the last production release on that branch.

Please see the file `CHANGES` for a more detailed list of changes and bug fixes.

1.2 Note on Version Numbering

As of BIND 9.13/9.14, BIND has adopted the "odd-unstable/even-stable" release numbering convention. BIND 9.14 contains new features added during the BIND 9.13 development process. Henceforth, the 9.14 branch will be limited to bug fixes and new feature development will proceed in the unstable 9.15 branch, and so forth.

1.3 Supported Platforms

Since 9.12, BIND has undergone substantial code refactoring and cleanup, and some very old code has been removed that supported obsolete operating systems and operating systems for which ISC is no longer able to perform quality assurance testing. Specifically, workarounds for UnixWare, BSD/OS, AIX, Tru64, SunOS, TruCluster and IRIX have been removed.

On UNIX-like systems, BIND now requires support for POSIX.1c threads (IEEE Std 1003.1c-1995), the Advanced Sockets API for IPv6 (RFC 3542), and standard atomic operations provided by the C compiler.

More information can be found in the `PLATFORM.md` file that is included in the source distribution of BIND 9. If your platform compiler and system libraries provide the above features, BIND 9 should compile and run. If that isn't the case, the BIND development team will generally accept patches that add support for systems that are still supported by their respective vendors.

As of BIND 9.14, the BIND development team has also made cryptography (i.e., TSIG and DNSSEC) an integral part of the DNS server. The OpenSSL cryptography library must be available for the target platform. A PKCS#11 provider can be used instead for Public Key cryptography (i.e., DNSSEC signing and validation), but OpenSSL is still required for general cryptography operations such as hashing and random number generation.

1.4 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.

1.5 Security Fixes

- A race condition could trigger an assertion failure when a large number of incoming packets were being rejected. This flaw is disclosed in CVE-2019-6471. [GL #942]
- **named** could crash with an assertion failure if a forwarder returned a referral, rather than resolving the query, when QNAME minimization was enabled. This flaw is disclosed in CVE-2019-6476. [GL #1051]
- A flaw in DNSSEC verification when transferring mirror zones could allow data to be incorrectly marked valid. This flaw is disclosed in CVE-2019-6475. [GL #1252]

1.6 New Features

- The new GeoIP2 API from MaxMind is now supported when BIND is compiled using **configure --with-geoip2**. The legacy GeoIP API can be used by compiling with **configure --with-geoip** instead. (Note that the databases for the legacy API are no longer maintained by MaxMind.)

  The default path to the GeoIP2 databases will be set based on the location of the **libmaxminddb** library; for example, if it is in `/usr/local/lib`, then the default path will be `/usr/local/share/GeoIP`. This value can be overridden in `named.conf` using the **geoip-directory** option.

  Some **geoip** ACL settings that were available with legacy GeoIP, including searches for **netspeed**, **org**, and three-letter ISO country codes, will no longer work when using GeoIP2. Supported GeoIP2 database types are **country**, **city**, **domain**, **isp**, and **as**. All of the databases support both IPv4 and IPv6 lookups. [GL #182]

- Two new metrics have been added to the **statistics-channel** to report DNSSEC signing operations. For each key in each zone, the **dnssec-sign** counter indicates the total number of signatures **named** has generated using that key since server startup, and the **dnssec-refresh** counter indicates how many of those signatures were refreshed during zone maintenance, as opposed to having been generated as a result of a zone update. [GL #513]

- A SipHash 2-4 based DNS Cookie (RFC 7873) algorithm has been added. [GL #605]

  If you are running multiple DNS Servers (different versions of BIND 9 or DNS server from multiple vendors) responding from the same IP address (anycast or load-balancing scenarios), you'll have to make sure that all the servers are configured with the same DNS Cookie algorithm and same Server Secret for the best performance.

- DS records included in DNS referral messages can now be validated and cached immediately, reducing the number of queries needed for a DNSSEC validation. [GL #964]

1.7 Bug Fixes

- When **qname-minimization** was set to **relaxed**, some improperly configured domains would fail to resolve, but would have succeeded when minimization was disabled. **named** will now fall back to normal resolution in such cases, and also uses type A rather than NS for minimal queries in order to reduce the likelihood of encountering the problem. [GL #1055]

- Glue address records were not being returned in responses to root priming queries; this has been corrected. [GL #1092]

- Interaction between DNS64 and RPZ No Data rule (CNAME *.) could cause unexpected results; this has been fixed. [GL #1106]

- **named-checkconf** now checks DNS64 prefixes to ensure bits 64-71 are zero. [GL #1159]

- **named-checkconf** could crash during configuration if configured to use "geoip continent" ACLs with legacy GeoIP. [GL #1163]

- **named-checkconf** now correctly reports a missing **dnstap-output** option when **dnstap** is set. [GL #1136]

- Handle ETIMEDOUT error on connect() with a non-blocking socket. [GL #1133]

- Cache database statistics counters could report invalid values when stale answers were enabled, because of a bug in counter maintenance when cache data becomes stale. The statistics counters have been corrected to report the number of RRsets for each RR type that are active, stale but still potentially served, or stale and marked for deletion. [GL #602]

- When a **response-policy** zone expires, ensure that its policies are removed from the RPZ summary database. [GL #1146]

1.8 License

BIND is open source software licensed under the terms of the Mozilla Public License, version 2.0 (see the `LICENSE` file for the full text).

The license requires that if you make changes to BIND and distribute them outside your organization, those changes must be published under the same license. It does not require that you publish or disclose anything other than the changes you have made to our software. This requirement does not affect anyone who is using BIND, with or without modifications, without redistributing it, nor anyone redistributing BIND without changes.

Those wishing to discuss license compliance may contact ISC at https://www.isc.org/mission/contact/.

1.9 End of Life

The end of life date for BIND 9.14 has not yet been determined. For those needing long term support, the current Extended Support Version (ESV) is BIND 9.11, which will be supported until at least December 2021. See https://www.isc.org/downloads/software-support-policy/ for details of ISC's 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/.